Information Technology

CYBERSECURITY

IRS Publication 4812

Contractor Security & Privacy Controls

Handling and Protecting Information and Information Systems

****This Publication Pertains to IT Assets Owned, Managed, or Operated by IRS Contractors ****

Publication 4812 (Rev. 12-2025) Catalog Number 54170T Department of the Treasury **Internal Revenue Service** www.irs.gov

Table of Contents

1.0 Background

The E-Government Act of 2002 (Public Law 107-347) Title III, Federal Information Security Management Act (FISMA) of 2002, as amended by Federal Information Security Modernization Act of 2014 (Public Law 113-283), requires each agency to provide security and privacy protection for "information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source". FISMA requires federal agencies to develop and implement policies for information security and privacy oversight of contractors and other users with access to federal information and information systems.

To ensure FISMA compliance, the National Institute of Standards and Technology (NIST) identifies specific security and privacy controls/criteria in NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. NIST provides a series of recommended security and privacy controls to be employed by agencies and service providers to ensure the confidentiality, integrity, and availability of federal information and information systems and guidelines for effective security controls that support federal operations and assets.

Because of requirements distinct to IRS mission objectives, as well as specific laws or rulings, such as 26 U.S.C § 6103, the Gramm-Leach Bliley (GLB) Act, the Federal Trade Commission (FTC) Financial Privacy Rule and Safeguards Rule, and the Sarbanes-Oxley Act, IRS contractors, their affiliates, subcontractors, and service providers are subject to additional requirements for protecting information and information systems, when appropriate or applicable.

By entering into a contract with the IRS, the contractor agrees to provide site access within 24 hours of receiving notification by the Contracting Officer's Representative (COR) or Contracting Officer (CO). Failure to allow access is considered a breach of contract terms and conditions, which could result in termination of the contract or assessment of liquidated damages as agreed to within FAR clause 52.211-11 - Liquidated Damages - Supplies, Services, or Research and Development (Sept 2000).

In signing a contract, the contractor agrees to provide the COR an updated Plan of Actions & Milestones (POA&M) monthly for any open findings identified during an on-site or virtual assessment conducted by the IRS. Failure to provide a POA&M to demonstrate how the contractor is addressing risks is a breach of contract terms and conditions, which will result in the COR withholding invoice approval until a POA&M is provided.

Refer to CA-5 (Plan of Actions and Milestones) and RA-5 (Vulnerability Monitoring and Scanning) for additional details on POA&Ms and vulnerability scanning reporting requirements.

2.0 Purpose

This publication defines security and privacy controls and requirements that apply to contractors, subcontractors, contractor personnel, and subcontractor personnel supporting the primary contract. Throughout this publication when security and privacy requirements are defined at the Contractor level they also flow down and apply to sub-contractor information systems. The information in this publication is based on the security and privacy controls framework under NIST SP 800-53 Rev. 5, where contractor employees have access to develop, operate, or maintain IRS SBU data. While NIST SP 800-53 Rev. 5, is a general guide, the intent of IRS Publication 4812 is to provide IRS privacy and security requirements specific to the IRS contracting environment.

This publication also describes the framework and general processes for conducting security and privacy assessments and responsibilities of the IRS and the Contractor in implementing security and privacy controls and safeguards to protect IRS SBU data and information systems.

As described in NIST SP 800-53 Rev. 5, "The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions and business functions with what the Office of Management & Budget (OMB) Circular A-130 defines as adequate security, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information".

3.0 Scope

The requirements in this publication and the security and privacy controls contained hereinafter are based on NIST SP 800-53 Rev. 5.

3.1. IRS Security and Privacy Controls Structure

NIST provides Federal agencies the flexibility to apply the privacy and security concepts and principles in NIST SP 800-53 Rev. 5 within the context of, and with due consideration to, each agency's mission, business functions, and environments of operation.

As part of its information security program**,** the IRS identifies security and privacy controls for the organization's information and information systems in IRS Publication 4812 – Contractor Security & Privacy Controls.

3.1.1 IRS Publication 4812 Applicability

IRS Publication 4812 identifies security and privacy controls specific to IRS contractor's information systems and IT environments. These controls are based on controls established in NIST SP 800-53 Rev. 5. IRS Publication 4812 contains IRS-specific requirements that meet the standard for NIST SP 800-53 Rev. 5, and the security and privacy controls, requirements, and standards described herein are to be used in lieu of the common, at-large security control standards enumerated in NIST SP 800-53 Rev. 5.

Note: All NIST Special Publication (800 series) are available at the following web site - https://csrc.nist.gov/publications/sp800.

IRS Publication 4812 defines basic security and privacy controls and requirements required of contractors, subcontractors, contractor employees, and subcontractor employees, in which contractor personnel or subcontractor personnel will either:

- Have information systems for tax administration purposes (or provide related services) outside of IRS facilities or outside of the direct control of the Service; and/or

- Have access to, compile, process, or store IRS SBU data on their own information systems or that of a subcontractor, or third-party service provider, that use their own information systems (or that of others) and Information, Communication, and Technology (ICT) (as defined in FAR Part 2) to access, compile, process, or store IRS SBU data while working at an IRS owned or controlled facility.

IRS Publication 4812 is incorporated by contract requirements language included in IRS contracts, agreements, and/or task orders (directly or through flow down provisions to subcontractors). IRS IT Security/FISMA requirements language is also included in any solicitations, contracts, or orders (directly or through flow down provisions) for IT acquisitions, which include hardware and/or software, telecommunications software or equipment, and maintenance and or/service (including consulting services) on any hardware

and/or software products. The most up-to-date IRS Publication 4812 is applicable to the contractor and subcontractors and is available on the IRS public website, irs.gov.

As used in this publication, the term "contract" unless specified otherwise, includes contracts, task/delivery/purchase orders, blanket purchase agreements, and interagency agreements in which IRS is the servicing agency and contractor services and resources, equipment, and systems are being used to support the contract, order, or agreement. This publication may also be used and incorporated into interagency agreements in which IRS is the requesting agency and the servicing agency does not have guidelines (or security and privacy controls consistent with NIST SP 800-53 Rev. 5 in place comparable to IRS Publication 4812).

As described in greater detail in subsequent sections, there are three baseline levels of security and privacy controls, networked environments, software development, and Cybersecurity Supply Chain Risk Management (C-SCRM). The specific security and privacy controls associated with each control level can be found in IRS Publication 4812, *Section 10.4*, and *Appendix C*. The use of baseline levels of security and privacy controls notwithstanding, IRS always reserves the right to add other controls to any given contract, order, or agreement to protect its assets and information based on the work being performed, the environment in which the work is being performed, perceived risks (threats and vulnerabilities), the suitability and effectiveness of existing controls, and other factors, as appropriate, in the best interest of the Government.

IRS Publication 4812 also describes the framework and general processes for conducting Contractor Security Assessments (CSA) to monitor compliance and assess the effectiveness of security and privacy controls applicable to any given contracting action subject to IRS Publication 4812.

4.0 SBU Data

The IRS defines Sensitive But Unclassified Information (SBU) Data as; "*any information which, if lost, stolen, misused, accessed, or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy which individuals are entitled under the Privacy Act"* (5 U.S.C. 552a).

SBU data includes but is not necessarily limited to:

Federal Tax Information (FTI), Personally Identifiable Information (PII), Protected Health Information (PHI), procurement sensitive information, system vulnerabilities, case selection methodologies, systems information, source code/software developed by the Contractor for the IRS, enforcement procedures, and investigation information.

Furthermore, live data, which is defined as production data in use. Live means that when changing the data, it changes in production. The data may be extracted for testing, development, etc., in which case, it is no longer live. Live data often contains SBU data.

Access to SBU data must be provided on a "need to know" basis. SBU data must never be indiscriminately disseminated, and no person must be given access to (or allowed to retain) more SBU data than is relevant and necessary for performance of their duties, and for which that individual has been authorized to receive because of having been successfully investigated, adjudicated, and trained to receive, and limited to what is strictly necessary to accomplish the intended business purpose and mission.

SBU data must only be released or accessible via access to information systems to those individuals who have been approved for interim/final staff-like access by IRS Personnel Security (see definition of staff-like access in Appendix B). Additionally, they should have a "need to know" to perform the work required under the contract.

SBU must be categorized in one or more of the following groups:

- FTI,
- Law Enforcement Sensitive (LES) information,
- Employee information,
- PII, and/or
- Other protected information.

4.1 Returns and Return Information

Returns and return information includes all information covered by § 6103 of the IRC, 26 U.S.C. § 6103. This includes tax returns and return information as defined by IRC, 26 U.S.C. § 6103(b).

4.2 Law Enforcement Sensitive (LES) Information

Law enforcement data is often sensitive in nature. This data falls under the data category called Law Enforcement, which includes grand jury, informant, undercover operations information, and procedural guidance.

4.3 Employee Information

All employee information covered by the Section 552a of Title 5, United States Code (USC) (5 U.S.C. 552A). Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams, and evaluation data.

4.4 Personally Identifiable Information (PII)

As defined in OMB Circular A-130: "Personally Identifiable Information" is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Since there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is broad. To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available in any medium and from any source that would make it possible to identify an individual.

Examples and categories of PII may include, but are not limited to the following, when used to distinguish or trace an individual's identity, or when combined with information that is linked or linkable to an individual:

- Name, such as full name, maiden name, mother's maiden name, alias, or name control (first 4 letters of last name).
- Address information, such as street address or email address.
- A unique set of numbers or characters assigned to a specific individual, such as:
    - Telephone numbers, including mobile, business, and personal numbers.
    - SSN or Individual Taxpayer Identification Number (ITIN), including the last 4 digits.

    - Taxpayer Identification Number (TIN) that identifies an individual, such as an Employer Identification Number (EIN) for a sole proprietorship or partnership.
    - Document Locator Number (DLN) to identify an individual's record.
    - Email or Internet Protocol (IP) address.
    - Driver's license number.
    - Passport number.
    - Financial account or credit card number.
    - Standard Employee Identifier (SEID).
    - Automated Integrated Fingerprint Identification System (AIFIS) identifier, booking, or detention system number.
    - Universally Unique Identifier (UUID), a unique random number generated for each individual taxpayer in the electronic authentication process (eAuth).
    - Any other type of identification number or card, including state ID or Alien Card ID.

- Employee and employee information, including personnel files, employment testing materials, medical information, and information concerning reasonable accommodations for disabilities.
- Individual tax return information, including Adjusted Gross Income (AGI) or combinations of fields that identify an individual.
- Corporate or other business tax return information that identifies an individual, such as an S-Corporation, partnership, or sole proprietorship.
- Personal characteristics and data, including:

    - Date of birth
    - Place of birth
    - Age
    - Height
    - Weight
    - Gender
    - Hair color
    - Eye color
    - Race
    - Ethnicity
    - Scars
    - Tattoos
    - Distinguishing features
    - Religious affiliation
    - Sexual orientation
    - Gang affiliation
    - Photographic image (especially of face or another distinguishing characteristic)
    - Biometric information (such as x-rays, fingerprints, retina scan, voice, facial geometry, DNA)
    - Behavior patterns

- Asset information, such as Media Access Control (MAC) address, Device ID, or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
- Descriptions of events or times (information in documents, such as behavior patterns, incident reports, police reports, arrest reports, and medical records).
- Descriptions of locations, such as Geographic Information System (GIS), Global Positioning System (GPS) data, and electronic bracelet monitoring information.
- Information identifying personally owned property, such as vehicle registration number or title number and related information.

4.5 Other Protected Information

Other protected information includes any knowledge or facts received or created by or for the IRS in support of IRS work. This includes all information covered by the Trade Secrets Act, the Procurement Integrity Act, and similar statutes. Examples include, but are not limited to:

- Records about individuals requiring protection under the Privacy Act.
- Information that is not releasable under the Freedom of Information Act (FOIA).
- Proprietary data.
- Procurement sensitive data, such as vendor contract proposals.
- Information, which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property, or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.
- Information related to the design and development of application source code.
- For contracting organizations providing IT services to the IRS, this includes specific IT configurations, where the information system security configurations could identify the state of security of that information system; IP addresses that allow the workstations and servers to be potentially targeted and exploited; and source code that reveals IRS processes that could be exploited to harm IRS programs, employees, or taxpayers.
- Security information containing details of serious weaknesses and vulnerabilities associated with specific information systems and/or facilities.
- Any information, which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission; and
- Information that would disclose techniques or procedures within the IRS not necessarily known to the public.

5.0 Information and Information Systems

Information requires protection whether or not it resides on an information system. Per OMB Circular A-130 (Section 6, Paragraph j), the definition of information is as follows:

The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information System, as defined by OMB Circular A-130, means “a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual”.

In all instances, security and privacy controls apply to both information and information systems.

6.0 Cloud Computing

Cloud computing is the delivery of computing services including but not limited to; Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This architecture differs from the widely used on premise IT model where the IT resources are physically housed, owned, and operated at contractor facilities by contractors.

In the Cloud Computing Model, IT resources are owned and operated by the CSP.

Some benefits of using a CSP include:

- Cost - Contractors do not need to buy hardware and software, or setup and manage their own datacenters.
- Speed and Performance - Contractors using a CSP are typical getting the latest hardware and software automatically when utilizing a CSP. Cloud computing services are on demand and can be provisioned for higher levels of performance immediately.
- Reliability - Cloud computing services operate across multiple geographic locations, High Availability and Redundancy are baked into the solution.

While there are many advantages to cloud computing there are some additional challenges to ensuring IRS SBU is protected in the Cloud. The CSA Team has incorporated language into IRS Publication 4812 to ensure that Contractors and subcontractors utilizing CSP's have security and privacy controls in place and functioning properly to protect IRS SBU, PII, and FTI.

Contractors that would like to implement Cloud computing services within their environments that support the IRS must contact the COR who will forward the request to the Contracting Officer and IRS Cybersecurity for review and approval. Contractors must not employ Cloud computing services to support the IRS contract without approval from the Contracting Officer and IRS Cybersecurity approval.

FTI may only be stored, processed, or handled in FedRAMP Authorized cloud environments operating at the Moderate or High impact level.

7.0 Artificial Intelligence

The term “artificial intelligence” or “AI” is defined in 15 U.S.C. 9401(3) as: “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs, to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action”.

The contractor must define an AI policy for any design, development, acquisition, or use of AI (hereafter referred to as AI use), whether a web-based online form, Commercial-off-the-Shelf (COTS) product or service, custom developed contractor tool, or any other use case. This policy applies to associated technologies that may not meet the IRS definition of AI. Examples of AI or associated technologies include:

- Generative AI
- Predictive AI
- Machine Learning (ML)
- Large Language Models (LLM)
- Voicebots and chatbots
- Robotic Process Automation (RPA)

Note: AI capabilities often appear as part of many other tools, applications or COTS products, without expressly being identified as AI.

Use of AI may create new security and privacy risks or exacerbate risks present in other systems. When using AI, contractors must consider the relationship between AI and security and privacy risks, such as collecting more data than is necessary, improper disclosure, misuse, data poisoning and even aspects of incorrect conclusions.

Contractors are strictly prohibited from disclosing Sensitive but Unclassified (SBU), to include PII and Federal Tax Information (FTI) information, to publicly available generative AI tools (e.g., ChatGPT, Google Bard/Gemini, Anthropic Claude). These open tools pose significant risks to data privacy and security, as well as the potential for biased, unpredictable, and malicious behavior. The IRS considers improperly sharing data with such an AI or internet tool as an intentional unauthorized disclosure and data breach. Contractors must not use IRS SBU data (including PII and tax information) to train public AI models.

Contractors are responsible for the information shared when using AI, just as they are responsible for the information shared in a conversation or email. This includes considering how the AI might use the information later.

Many AI models can intake, keep, and reuse data. Under the IRS policies for minimization, minimize the collection, use, retention, and disclosure of data in AI to what is specifically

relevant and necessary. The Contractor must take steps to understand how AI might redisclose data and share only what is necessary for your task. When developing an AI model, the contractor must build in safeguards that guide users how to minimize data and to prevent improper disclosure.

Contractors and subcontractors that would like to implement AI technologies within their environments that support the IRS must receive approval by the CO before implementing AI. Contractors and subcontractors must not employ AI technologies to support the IRS contract without consultation with IRS Cybersecurity and approval from the Contracting Officer.

8.0 Unauthorized Access (UNAX) and Disclosure of Information

IRC Section 26 U.S.C. § 7213A makes the unauthorized inspection of returns and return information a misdemeanor punishable by fines, imprisonment, or both. IRC Section 26 U.S.C. § 7431 allows for civil damages for unauthorized inspection or disclosure of returns and return information, and upon conviction, the notification to the Taxpayer that an unauthorized inspection or disclosure has occurred.

Disclosure of returns and return information is generally prohibited unless authorized by statute. Returns and return information are defined by IRC, 26 U.S.C. § 6103(b). The IRC makes the confidential relationship between the taxpayer and the IRS quite clear, and stresses the importance of this relationship by making it a crime to violate this confidence. Designed to protect the privacy of taxpayers, IRC Section 26 U.S.C. § 7213 prescribes criminal penalties for contractors and their employees who make unauthorized disclosures of returns and return information. The sanctions of the IRC are designed to protect the privacy of taxpayers.

IRC Section 26 U.S.C. § 6103 (n) gives the contractor the authority to disclose returns and return information to its employees whose duties or responsibilities require the returns and return information for a purpose described in paragraph (a) of the section. Prior to releasing any returns and return information to a subcontractor, the Contractor must have written authorization from the IRS.

Contractors and subcontractors must have adequate programs in place to protect the information received from unauthorized use, access, and disclosure. The Contractor's programs for protecting information received must include documented notification to employees and subcontractors (at any tier) regarding, the importance of protecting returns and return information. The documented notification must also include the disclosure restrictions that apply and the criminal or civil sanctions, penalties, or punishments that may be imposed for unauthorized disclosure or inspection. Disclosure practices and the safeguards used to protect the confidentiality of information entrusted to the Government, as provided under the IRC are subject to continual assessment and oversight to ensure their adequacy and efficacy.

9.0 Roles and Responsibilities

The following sections define roles and responsibilities in the contractor assessment process.

9.1 IRS

9.1.1 Contracting Officer (CO)

- Enforces the Government's rights and remedies for all contractual matters.
- Ensures compliance with the terms and conditions of the contract.
- Ensures appropriate privacy and security-related clauses and language are included in applicable contracts with coordination from the CSA Team and the Privacy Governmental Liaison and Disclosure (PGLD) Team.
- Ensures the contractor affords the Government access to the contractor's facilities, installations, operations, documentation, records, IT systems, and databases to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of government data.
- Employs all rights and remedies available to the Government to ensure contractors correct or mitigate identified security vulnerabilities.
- Modifies the contract, when risk level requires modification, based upon the CSA and PGLD Team recommendations.
- Assists with reporting and mitigation of incidents as appropriate. (See section 20.6 IR-6 Incident Reporting.)

9.1.2 Contracting Officer's Representative (COR)

- Facilitates CSAs and serves as the liaison between the CSA Team and the contractor when scheduling CSAs and by being the primary IRS point of contact for the contractor.
- Escalates key information to the CO related to contractor risk.
- Provides a monthly status of all related POA&Ms to the CSA, PGLD, and Facilities Management and Security Services (FMSS) Teams.
- Furnishes CSA, PGLD, and FMSS Team documents to the contractor.
- Identifies to the contractor, the names of specialized IT security roles and the associated number of required hours for Specialized Security Training (SITs).
- Ensures all security awareness, privacy, records management, and physical environment mandatory briefings assigned to each contractor are completed, recorded in the IRS learning system, and within the IRS required timeframe for completion.
- Serves as the liaison between (PGLD) and the contractor. If entering into a data sharing agreement with a contractor, or vendor that involves custody of, or access to IRS-held PII that will be collected, maintained, or disseminated using IT, work with the contractor to complete a Privacy Threshold Assessment (PTA) to document and identify any additional privacy compliance requirements. A PTA can be used to determine whether a full Privacy & Civil Liberties Impact Assessment (PCLIA) is required.

- Ensures (when applicable) the completion or update of a PCLIA in the Privacy Impact Assessment Management System (PIAMS). For any PCLIAs that will expire at the end of the contract, or after three years from issuance, whichever comes first, the COR must:
    - Email PGLD.Contractor.Privacy.Assessment@irs.gov and privacy.review@irs.gov for instructions on renewing a PCLIA.
    - Ensure all contractors and subcontractors with staff-like access to SBU data are properly investigated prior to being given access.
    - Assist with reporting and mitigation of incidents as appropriate. (See section 20.6 IR-6 Incident Reporting.)

9.1.3 Contractor Security Assessment Team (CSA)

- Establishes the schedule for CSAs, in coordination with COs, CORs, and contractors.
- Conducts on-site or virtual CSAs.
- Coordinates with the COR to identify contractor security review timeframes to conduct assessments.
- Provides CSA documents to the COR, CO, and the Security Program Management Office. The CSA documents include:

    - Executive Memorandum - that includes the Contractor IT and privacy environment, physical description of the site, and significant security, physical security, and privacy findings.
    - Findings Report - which is a PDF version of the findings found during the assessment in a tabular format listing the security control, justification for the finding, and recommendation to resolve the issue/finding, and
    - Data Collection Instrument (DCI) - PDF versions of the DCI completed during the on-site/virtual assessment which detail the observations of the CSA Team.

- Maintains and updates, as appropriate, IRS Publication 4812 and coordinates changes or updates with IRS stakeholders.
- Acts as a resource for CORs/ Business Operating Divisions (BODs) in developing POA&Ms and assessing compliance, and reconciliation or mitigation efforts.
- Acts as a Point of Contact (POC) for technical issues for BODs and Procurement Officials (and directly or indirectly for contractors).
- Alerts Computer Security Incident Response Center (CSIRC) and/or Situation Awareness Management Center (SAMC) of any potential or suspected incidents, risks, or vulnerabilities discovered while conducting a Contractor Security Assessment, that represent immediate, actionable threat intelligence, or presents an unusually urgent demand for attention, correction, or remediation. Similarly, alerts Disclosure, FMSS, Procurement, PGLD, or others, as appropriate, of issues of a pressing nature revealed while conducting a CSA that falls within each component's areas of responsibility.

9.1.4 Privacy, Governmental Liaison and Disclosure (PGLD)

PGLD is responsible for safeguarding and protecting sensitive taxpayer and employee information, while promoting government transparency and accountability through better access to government information. Questions about privacy can be routed through the COR and sent to PGLD.Contractor.Privacy.Assessment@irs.gov and privacy.review@irs.gov mailbox.

To accomplish its mission, PGLD:

- Preserves and enhances public confidence by advocating for the protection and proper use of sensitive information.
- Protects the sensitive information and privacy of taxpayers and IRS employees.
- Reduces vulnerabilities for identity theft, which promotes identity protection.
- Ensures IRS records (hard copy and electronic), including those containing PII, are managed appropriately and in accordance with the Records Control Schedules (RCS) Document 12990 and General Records Schedules (GRS) Document 12829.
- Analyzes, and resolves incidents involving the loss or theft of an IRS asset, or the loss, theft, destruction, or disclosure of PII.
- Works with all IRS operations to ensure only authorized disclosures and data sharing.
- Partners with federal, state, tribal, territorial, and local governmental agencies to promote privacy and protect FTI.
- Exchanges FTI as authorized by law with external stakeholders.
- Safeguards FTI held by data exchange partners.
- Protects IRS employees with cautionary indicators on appropriate taxpayer accounts.
- Processes requests for agency records requested under the FOIA Title 5 U.S.C 552.
- Create and track POA&Ms for PGLD findings.
- Collaborates with the CSA Team to conduct the privacy assessment.

9.1.5 Facilities Management and Security Services (FMSS)

- Trains and supports IRS employees and contractors to adequately protect locations and sensitive information where IRS work is performed (FMSS Physical Security).
- Prepares and disseminates SAMC Incident Reports accordingly.
- Collaborates with the CSA Team to conduct the physical security assessment.
- Creates and tracks POA&Ms for physical security findings.

9.1.6 Personnel Security (PS)

- Receives and processes all investigative requests from the COR.
- Responsible for determining eligibility and suitability for all contractor employees who require staff-like access to IRS facilities, systems, or SBU data.
- Notifies the appropriate IRS stakeholders of any changes to access status.
- Intakes and assesses Position Designation Surveys from contractors (directly or through the COR) and uses the Office of Personnel Management Position Designation Tool

(PDT) to assign the position risk designation (or make adjustments/updates, as needed) prior to granting contractor personnel interim or final staff-like access to IRS information or information systems.

9.2 Contractor

To ensure IRS SBU and information systems are protected, it is the responsibility of IRS contractors to develop and implement effective controls and methodologies in their business processes, physical environments, and human capital or personnel practices that meet, or otherwise adhere to the security and privacy controls, requirements, and objectives described in this publication, and their respective contracts. As part of the award process, the contractor is required to include an assigned Vendor POC and alternate Vendor POC to all contracts requiring access to Treasury/Bureau information, IT, and systems, facilities, and/or assets. The Vendor POC is the contractor's primary POC for the Government on all privacy and security-related matters and the person responsible for ensuring the security of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls.

The Contractor is responsible for protecting IRS SBU data (including PII and FTI) based on the contract, the PCLIA, and the privacy and security controls defined in this publication.

9.2.1 Contractor Point of Contact (POC)

Within 5 calendar days of contract award or order issuance, the Contractor POC must submit to the COR a list of contractor employees who will have a significant role or responsibility for IT security, in the performance of the contract, including those authorized to handle IRS SBU. The Contractor POC will identify the specific IT security role the employee will perform under the contract and will indicate whether such employee(s) has/have completed role-based training, as well as the source and title/subject of the training.

Significant responsibilities must include but may not be limited to contractor employees who have access to either contractor-managed facilities or contractor managed systems/IT assets used to handle, process or store IRS SBU data, regardless of location or facility, to include contractors who need such access including the use of other IT resources, at contractor managed facilities.

The Contractor POC is responsible for ensuring the following responsibilities are addressed through the life cycle of the contract:

- Provide monthly updates to the COR for all findings using a POA&M
- Report all incidents to the IRS, as required under the Incident Reporting section of this document.
- Ensure all employees undergo the necessary security screening process and receive interim or final staff-like access approval prior to beginning work under the awarded contract or order, and
- Ensure all contractor employees take required IRS SAT training within five business days of being granted interim/final staff like access and annually thereafter for all IRS required training.

9.2.2 Contractor Personnel

- Ensure all required IRS training is completed within five business days of being granted interim/final staff like access and annually thereafter.
- Ensure all privacy, physical, and security policies and procedures are followed when supporting the IRS contract.
- Ensure the safeguarding of all information provided to the contractor as part of the IRS contract.

9.3 Contractor Program Requirements

The Contractor must develop a comprehensive security program that addresses all aspects of IT security and privacy.

9.3.1 Contractor Security Policies and Procedures

Contractors and subcontractors are responsible for developing policies and procedures to implement security and privacy controls and requirements, as established by this publication and the contract.

As described in NIST SP 800-53 Rev. 5, the first security control in each family is also known as the "*dash one"* control (e.g., AC-1, CP-1, SI-1, etc.). It generates the requirement for policy and procedures that are needed for the effective implementation of security and privacy controls and control enhancements in the family.

A contractor or subcontractor who is subject to the security and privacy controls under IRS Publication 4812 does not necessarily have to develop a plan specific to each family if and when those policies and procedures are already established in some existing formal or institutional document that the contractor can readily identify (to the satisfaction of IRS), and the plan contains policies and procedures that address the material elements or requirements for that particular dash one control and security and privacy control family. For example, if the Personnel Security Policy and Procedures (PS-1) requirements for a formal documented PS policy (and procedures to implement those polices and associated personnel security controls) are already contained in the Contractor's existing Human Resources (HR) policies, the Contractor would not have to recreate this documentation so long as the IRS determines (or is in a position to determine) these existing products or records fulfill the key, germane aspects and requirements for that particular dash one control, as specified in IRS Publication 4812.

Only when the Contractor or Subcontractor does not have standing policies and procedures that adequately and fully address each respective security and privacy control family's dash one requirement (or the existing policies and procedures are inadequate and need to be supplemented), does the contractor need to develop specific policies and procedures to address that control family.

9.3.2 Contractor Investigative Requirements

Contractors, subcontractors, experts, consultants, and paid/unpaid interns, like federal employees, are subject to a security screening to determine their suitability and fitness for the Department of the Treasury or IRS work, and the security screening must be favorably adjudicated. The level to which such contractor personnel and others are screened or investigated must be comparable to that required for federal employees who occupy the same positions and who have the same position sensitivity designation. Security screening is required regardless of the location of the work. This includes contractor or subcontractor employees who use technology for remote access to information technology systems, as well as those who have direct physical access to any IRS documents or data outside of any IRS facility.

The Vendor POC, in collaboration with the COR, must ensure all contractor and subcontractor employees performing or proposed to perform under the contract as well as those meeting the definition of the term staff-like access are identified to the IRS at time of the award (or assignment) to initiate appropriate security screening.

Working collaboratively, the Vendor POC, the COR, and the CO must ensure that any personnel who are not favorably adjudicated or otherwise pose a security risk are immediately removed from performing work under contract with the IRS, and suitable replacement personnel agreeable to the IRS are provided.

9.3.3 Contractor Training

Ensure all contractor and subcontractor employees who require staff-like access to IRS information or information systems regardless of their physical location complete the required Security Awareness Training (SAT) prior to being granted access to SBU data.

As of July 2025, IRS has developed a methodology to assign the following mandatory briefings to all individuals supporting IRS contracts:

- Annual Cybersecurity Awareness, Privacy, Information Protection & Disclosure (PIPD),
- Records Management,
- Insider Threat Awareness,
- FMSS Physical Security,
- IRS Cybersecurity Awareness,
- Inadvertent Sensitive Information Access,
- Controlled Unclassified Information (CUI) General Awareness, and
- UNAX.

Maintain and furnish, as requested, records of initial and annual training and certifications. Establish additional internal training, as needed (or as required under the terms of the contract), for personnel in the organization who require access to IRS SBU or information systems to perform under the contract.

Reference AT-2 Security and Awareness Training for time requirements to complete training.

9.3.4 Contractor Information Protection

Ensure all SBU data is protected at rest, in transit, and in exchanges (i.e., internal and external communications). Limit access to SBU data to authorized personnel (those favorably adjudicated and trained) with a need to know and ensure internal and external exchanges are conducted only through secure or encrypted channels. The Contractor and Subcontractor must employ encryption to ensure the confidentiality, integrity, and availability of the SBU data, consistent with the security controls under IRS Publication 4812 and any additional security requirements specified in the contract.

9.3.5 Rules of Behavior

Contractors and subcontractors must develop and distribute a set of internal Rules of Behavior regarding access to and the use of government information and information systems. Rules of Behavior, which are required in OMB Circular A-130, Appendix III, and is a security control contained in NIST SP 800-53 Rev. 5, must clearly delineate responsibilities, and expected behavior of all individuals with access to information systems and/or government information and/or IRS SBU data. The rules must state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system and/or IRS SBU data. It is required that the rules contain a signature page for each user to acknowledge receipt; indicating that they have read, understand, and agree to abide by the Rules of Behavior. Electronic signatures are acceptable for use in acknowledging the Rules of Behavior. Contractors must maintain (and furnish, as requested) records of signed acknowledgements on the Rules of Behavior, Non-Disclosure Agreements (NDAs), and the completion of all required awareness training.

10.0 Contractor Security Assessments

10.1 Overview

Security and privacy controls are the management, operational, and technical safeguards or countermeasures employed to protect the confidentiality, integrity, and availability of an organization's information and information systems.

CSAs are on-site or virtual evaluations performed by the IRS to assess and validate the effectiveness of security and privacy controls established to protect IRS SBU data and information systems. Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to protecting information and individual privacy, or meeting the security requirements for the information system in its operational environment. These assessments help to determine if additional controls or protections are necessary to protect returns, return information, personal privacy, other SBU data, and organizational assets and operations.

All contracts subject to this publication, may be required to undergo an on-site or virtual CSA annually.

10.2 Types of Assessments

Current contract conditions and the stage of the acquisition lifecycle will dictate the type of CSA the IRS will perform. Qualifying events or conditions that may prompt or necessitate the IRS to perform a CSA include:

- Pre-Award Assessments: Pending the award of a contract, an IRS Business Unit (BU) may request a Pre-Award Assessment to determine the security profile of a contractor. Results of such assessments may be used as an element of the contractor selection process.
- Post–Award Assessments: This type of assessment is conducted within the first 30 to 90 days of award and may be performed in lieu of a pre-award assessment when award is imminent and the need to make the contract award is urgent and compelling but conducting a pre-award assessment is not viable. In such cases, an assessment is necessary as soon as possible after the contract is awarded to approve interim access to IRS SBU.
- Periodic Assessments: Based upon the type of work being performed and the volume of SBU data being processed, the IRS may schedule an assessment, at least annually, to ensure security controls are in place, and operating as intended.
- Follow-up Security Assessment: Based upon the magnitude of findings identified on an assessment, a follow-up assessment may be warranted to evaluate remedial actions taken to address identified security issues.
- End of Contract Assessments: At contract expiration or termination, the IRS may elect to conduct a security assessment to ensure that all IT resources and SBU data have been adequately inventoried and returned or disposed of in accordance with the contract.

10.3 Notice of Assessments

For each contract the IRS selects for assessment, in any annual assessment cycle, the IRS will advise the Contractor of the intent to conduct an on-site or virtual CSA and the projected timeframe or proposed date of the assessment. The IRS will coordinate the logistics for the upcoming assessment and advance notice is as much a courtesy as it is recognition of the planning and preparations required by both the IRS and the Contractor.

Typically, an on–site or virtual CSA is three days in duration.

10.4 Security Control Levels

Contractor sites and work environments using IT assets to access, process, manage, or store IRS SBU data under contract to the IRS will likely vary in size, number of users, and complexity. For this reason, the IRS has established minimum and advanced sets of security controls that are selected, depending upon the complexity of the contract, cost, and other factors. As described in more detail in the following subparts, three control sets are categorized (within the assigned moderate impact designation) as follows:

- Networked Information Technology Infrastructure (NET),
- Software Application Development or Maintenance (SOFT),
- Cyber Supply Chain Risk Management (C-SCRM)

Scope: The defined conditions for determining and applying security control levels/security controls are as follows (in descending order of precedence and logical progression):

- Development Activity (highest operator): Contracts that involve software or application development, design, maintenance, configuration, or related support services.
- IT System Environment: A contractor that operates in and/or houses IRS information on a contractor network environment infrastructure, and
- Security Control Levels: IRS Publication 4812 employs the following three security levels (within the assigned impact designation applicable contracting actions, which are moderate, by default).

Networked Information Technology Infrastructure (NET)

Contracting actions for services that involve contractor access to SBU data and/or information systems, by any contractor (individual or business concern) that has a networked IT infrastructure (in short, an interconnected group of computer systems linked by the various parts of telecommunications architecture).

Examples of a networked infrastructure include: IRS SBU is maintained on a file or shared area, where access controls are used to manage access to the file or shared area, or IRS SBU is maintained on a file that is shared among multiple employees who all have authority and need to know to access and maintain the information.

Software Application Development/Maintenance (SOFT)

Contracting actions for services that involve contractor access to SBU data and/or information systems, by any contractor (individual or business concern) that entails software application development, maintenance, configuration, or related support service.

An example of this type of contract or environment includes contractor sites, where multiple employees have access to IRS SBU data and/or IT assets and where this information is being accessed on information systems in a networked environment. In addition, the contractor is providing support to develop software, perform testing, configure, and perform information system maintenance or other related support service.

Cyber Supply Chain Risk Management (C-SCRM)

C-SCRM refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. C-SCRM addresses threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself.

Examples of these risks include:

- Insiders working on behalf of a system integrator steal sensitive intellectual property, resulting in the loss of a major competitive advantage.
- A proxy working on behalf of a nation-state inserts malicious software into supplier-provided product components used in systems sold to government agencies. A breach occurs and results in the loss of several government contracts.
- A system integrator working on behalf of an agency reuses vulnerable code, leading to a breach of mission-critical data with national security implications, and
- An organized criminal enterprise introduces counterfeit products onto the market, resulting in a loss of customer trust and confidence.

The C-SCRM controls and supplemental guidance within this publication provides guidance on requirements and mitigating controls to help manage cybersecurity risks throughout the supply chain. **Note: C-SCRM controls and Supplemental C-SCRM Guidance within this publication will be assessed by the C-SCRM team during C-SCRM assessments and not during Contractor Security Assessments.**

10.5 Scope of Assessments

CSAs typically address the following key areas:

- Information and information systems.
- The physical environment in which the information system or systems resides, and/or where the information is handled, or processed.
- Personnel who have access to or are responsible for the handling or processing of information and information systems.
- Evaluation of all applicable IRS Publication 4812 security and privacy controls.

- Verification of all personnel security background investigations or interim/final staff-like access determinations for all contractor employees working on the IRS contract, including subcontractor employees, and IT support personnel (at any tier) who have unescorted staff-like access to IRS facilities, SBU data, and/or information systems.
- Validation of IT security configurations including, but not limited to, workstations, servers, routers, and switches.
- Verification of employee's completion of IRS mandated SAT, which is based on the completion of various information protection briefings 5 days from being granted interim/final staff like access, and annually thereafter on information system security, disclosure, privacy, physical security, and/or UNAX – commensurate with the assigned risk designations of the position for the work being performed and the category of SBU data to which the employee has access.
- Vulnerability and configuration (compliance) scans, and
- Preliminary identification of any weaknesses, threats, or vulnerabilities, with more details to be provided in later CSA documentation.

10.5.1 Collaboration on Contractor Security Assessment

10.5.1.1 Before the Assessment

Contractors must coordinate with the IRS on all aspects of preparation for the assessment to include but not limited to; agreement on time and location of assessment, timely submission of any pre-site visit materials, making ready for inspection- policies, documentation, configurations, and records required at the time of the assessment.

10.5.1.2 At the Time of or During the Assessment

Contractors must make its facilities, installations, operations, documentation, records, databases, and personnel available to the IRS to carry out a program of inspection (in a manner not to unduly delay the work) to protect against threats and hazards to the security, confidentiality, integrity, and availability of IRS data.

Access to contractor facilities and IRS information and/or information systems by IRS representatives (e.g., CORs and CSA Team) must be permitted, in accordance with the terms of the contract, subject to confirmation of identity, which must be based on each person presenting an active (unexpired), government issued Personal Identity Verification (PIV) card. PII such as a Driver's License, SSN or Date of Birth (DOB) must not be requested of government personnel conducting an assessment.

A contractor facility that maintains classified information, is subject to the National Industrial Security Program, and has additional government mandated protocols for access, must identify those requirements in writing to the IRS, for its consideration, not less than 10 days before the scheduled inspection/assessment. Denial of access to the Government to conduct its inspections may violate the terms of the contract and constitute a breach of contract.

10.5.1.3 After the Assessment

Within 90 days of the completion of the CSA, the CSA Team must furnish to the CO/COR the final CSA documents who will share the results with the Contractor

The CSA documents contain the results of the security assessment. This typically includes:

- Findings of "not met" or "repeat not met" (with respect to not meeting individual security controls standards/requirements).
- Identifying the parts of the security controls that did not produce a satisfactory result, or may have the potential to compromise IRS SBU, or the contractor's information system.
- An evaluation on the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- An assessment on the organization's overall effectiveness in providing adequate security, and
- Recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities.

The Findings Report is a key element used in developing a Plan of Actions & Milestones (POA&M). The POA&M is a management process and tool developed by the IRS that outlines weaknesses or deficiencies identified in the CSA and delineates the tasks necessary to correct, remediate, or mitigate less than satisfactory findings.

The Contractor must collaborate with the IRS to prioritize the identified weaknesses/deficiencies for corrective actions and identify the actions to be taken within an agreed upon, realistic schedule (within the period of performance or life of the contract) to correct or effect desired changes in any weaknesses or deficiencies identified in the Findings Report. The Contractor must track and furnish monthly POA&M updates to the IRS COR.

10.5.2 Continuous Monitoring of Security and Privacy Controls

Contractors must maintain ongoing awareness of their information system and related security and privacy control processes to ensure compliance with security and privacy controls and adequate security of information, and to support organizational risk management decisions.

11.0 Privacy and Information Protection

11.1 Security Categorization

The Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, establishes security categories for both information and information systems. The information system impact level is derived from the security category in accordance with FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. FIPS 200 and NIST SP 800-53 Rev. 5, in combination, help ensure that appropriate security requirements and controls are applied to all federal information and information systems.

As required by FIPS 199, organizations use the security categorization results to designate information systems as low, moderate, or high impact.

The IRS has determined the security impact for all contracting actions subject to IRS Publication 4812 is moderate impact, unless:

- The information system in the contract to which the Contractor has staff-like access is one of the limited number of systems on the IRS FISMA Inventory (i.e., it is specifically identified as such, and/or it is a major application or general support system, as defined by OMB Circular A-130, Appendix III). In this case, IRS Publication 4812 would be replaced with the more stringent standards for a high impact system, and other requirements as may be specified by IRS.
- A different impact level is specified in the contract (at time of award, or by modification).

The security impact level can only be lowered when IT Cybersecurity determines, in writing, all three of the security objectives (confidentiality, integrity, and availability) are low. The security impact level must only be raised if IT Cybersecurity determines, in writing, one or more of the three security objectives is high.

In the event the impact level is to be lowered or raised from moderate impact for any contract that is subject to IRS Publication 4812, the change must be reflected in the contract at time of award or by modification of the contract. At such time, security control requirements appropriate to the new impact level must be provided to the contractor (e.g., guidance on any security controls or control enhancements from the default standard (moderate-impact) that do not apply (or are lessened), if and when the impact level is being lowered to low-impact; or additional controls or control enhancements above the default standard (moderate-impact) that would apply, if and when the impact level is being raised to high-impact.)

12.0 Security and Privacy Control Organization and Structure

This document provides required controls for protecting SBU data, developed from NIST guidance. The security controls in this document are organized into families as described in NIST SP 800-53 Rev. 5. Each security control family contains security controls related to the functionality of the family. A two-character, unique identifier is assigned to each security control family.

The following table summarizes the control families and associated identifiers for developing security and privacy controls used in this publication.

Table 1: NIST Families of Security and Privacy Controls

IDENTIFIER	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	PII Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

The twenty security control families in NIST SP 800-53 Rev. 5 are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family, Program Management (PM) provides controls for information security programs. PM, while not referenced in FIPS 200, provides security and privacy controls at the organizational level rather than the information system level. The PM controls address the strategic level implementation of an overall security and privacy program. Contractors subject to IRS Publication 4812 are not responsible for the implementation of IRS strategic security PM but are required to abide by PM Privacy controls in IRS Publication 4812.

13.0 Access Control (AC)

The AC family provides security controls required to restrict access to IRS SBU data and information systems. IRS SBU data must be restricted to contractors that have been approved for interim/final staff-like access by IRS PS and have a "need-to-know".

13.1 AC-1 Access Control Policy and Procedures

Contractors, including those using a CSP, who have IT assets (i.e., information systems or servers), must ensure that they or the CSP designate an official to manage the development, documentation, and dissemination of the AC policies and procedures for security and privacy related controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organizational Entities
- Compliance

Contractors and CSP's must review/update AC policies and procedures annually or if there is a significant change to ensure adequate AC policies and procedures are developed and implemented.

Supplemental C-SCRM Guidance: Contractors must specify and include in agreements (e.g., contracting language) AC policies for their suppliers, developers, system integrators, external system service providers, and other Information and Communication (ICT) /Operations Technology (OT) related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.2 AC-2 Account Management

The Contractor or CSP shall create a unique account for each user who accesses the information system.

The Contractor or CSP shall assign an account manager to manage accounts and employ automated mechanisms to support the management of accounts. Automated mechanisms include helpdesk software, email, telephone, and text messaging notifications.

There must be a procedure that describes how accounts must be established and reviewed at least annually (semi-annually for privileged accounts), modified, or deleted, as necessary. At a minimum, the Contractor must identify all personnel authorized to access the IT asset, including information system support personnel.

The Contractor must notify account managers:

- When accounts are no longer required,
- When users are terminated or transferred, and
- When individual information system usage or need-to-know changes.

The Contractor or CSP must automatically disable all user accounts after 60 days of inactivity. The Contractor must disable any account within one hour if the user poses a serious security or privacy risk, either by planning to misuse access or by being vulnerable to exploitation by adversaries.

The Contractor must disable accounts within 3 business days when the accounts have expired or are no longer associated with a user. The information system must automatically remove/terminate temporary and emergency accounts after two business days.

The information system must automatically audit account creation, modification, enabling, disabling, and removal actions and notify, as required, the appropriate individuals.

Call recording systems must restrict access to staff initiating or receiving calls and staff members performing a quality assurance function.

Supplemental C-SCRM Guidance: Contractors must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts must only be established for appropriately vetted contractor personnel. Contractors must also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.3 AC-3 Access Enforcement

Contractors including those using a CSP, must ensure that they develop a process that demonstrates how employees are approved for access, prior to being granted authorized access to information systems used for IRS work. The contractor must develop policy directing taxpayers to the IRS for any inquiries, access requests, or requests to modify their PII.

Supplemental C-SCRM Guidance: Contractors must ensure that their information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Contractors must ensure that a defined consequence framework is in place to address AC violations. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.4 AC-4 Information Flow Enforcement

Contractors including those using a CSP, must ensure that they implement information flow enforcement. Contractor information systems must enforce approved authorizations for controlling the flow of information within the system and between connected systems based on applicable policies, agreements, contracts, and/or procedures. Examples of information flow control restrictions include keeping export-controlled information from being transmitted in the clear to the internet; blocking outside traffic that claims to be from within the organization; restricting web requests to the internet that are not from the web proxy server; and limiting information transfers between organizations based on data structures and content.

Supplemental C-SCRM Guidance: Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the Contractor and its various clients, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements and how information flow is enforced should ensure that only the required information is communicated to various participants in the supply chain. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Contractors, including those using a CSP, must ensure that they establish appropriate division of responsibilities and separation of duties to prevent harmful activity without collusion, so that no individual must have all necessary authority and system access to disrupt or corrupt a security process.

Supplemental C-SCRM Guidance: Contractors must ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the Contractor's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.6 AC-6 Least Privilege

Contractors, including those using a CSP, must ensure that contractor personnel have only privileges required to perform their specific duties.

The Contractor must authorize access to security functions. Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, running, and reviewing security scans, establishing intrusion detection parameters, system programming, system and security administration, other privileged functions.

The Contractor must require that users of system accounts or roles with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

The Contractor must prohibit non-privileged users from executing privileged functions. Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities.

The Contractor must restrict privileged accounts on IT assets, applications, and databases to only those personnel who require access to perform job functions. The configuration of the IT environment must be controlled so that non-privileged users cannot access and/or perform privileged roles.

All actions performed on the system using privileged roles must be audited to deter, detect, and report on potential misuse. The Contractor must log the execution of all privileged functions to assist in mitigating the actions of an insider threat or for detection of compromised privileged accounts.

Accounts with administrative privileges (including local administrator rights) must be prohibited from web browsing, internet connections, and accessing email. This shall be implemented by establishing separate accounts for privileged users. One account with administrative rights for privileged duties and a standard user account without administrative rights for routine business functions.

FTI, PII and IRS SBU data must be physically or logically partitioned within the information system and/or the IT environment, to ensure this sensitive information is not commingled with the information of any other entity and is accessible only to authorized personnel. Partitioning can be accomplished with the use of routers and firewalls and directories controlled by user permissions. Workstations shall be configured to restrict logical access to IRS SBU.

Contractors must restrict the following activities, privileges, and processes for non-administrative users:

- Administrative tools, including Event Viewer, and information system utilities.
- Command line access.

- Ability to install software, including adding, removing, or modifying software, unless this is part of the individual's job responsibilities.
- Access to insecure protocols such as FTP or Telnet.
- Local administrator rights on workstations.
- Backup rights to either the information system and/or server.
- Elevated access rights to the database software, and
- Saving files to either an electronic, optical, or other removable media including USB devices must be disabled.

13.7 AC-7 Unsuccessful Login Attempts

The Contractor must configure their information system to lock an account after 3 unsuccessful logon attempts in a 120-minute period. Once an account is locked it must remain locked for 15 minutes or until released by an administrator or password reset program.

Contractors using a CSP must ensure that, upon a 3rd unsuccessful logon attempt during a 15-minute time-period, the CSP will lock the account for a minimum of 30 minutes or until unlocked by an administrator and delay the next logon prompt, at a minimum for five seconds.

13.8 AC-8 System Use Notification

Contractors, including those using a CSP, must display an interactive system use notification with a privacy and security notice before granting access.

The system use notification must be reviewed and signed by the Contractor's legal counsel or designated individual.

The system use notification must state:

- The use of the information system indicates consent to monitoring and recording.
- Information system use is monitored, recorded, and subject to audit, and
- Unauthorized use of the information system is prohibited and subject to disciplinary actions.
- Sanctions and penalties for system misuse.

For publicly accessible applications or web hosting environments requiring user registration, the application or hosting environment must:

- Display the information system use information before granting further access.
- Display references to monitoring, recording, or auditing that are consistent with privacy accommodations for such information systems that generally prohibit those activities, and
- Include a description of the authorized uses of the system.

13.9 AC-11 Device Lock

When a contractor uses an IT device for IRS work, it must be locked when the device is left unattended. When a device lock is established, the device or application must remain locked until the user provides valid identification and authentication information. The device lock must take effect whenever the information system or application is left inactive for 15 minutes.

When the device lock is implemented, a generic screen saver must be displayed in lieu of the information previously being processed.

Contractors using a CSP must ensure that the CSP initiates a device lock after 15 minutes of inactivity and retain the device lock until the user provides valid identification and authentication to re-enter the session.

13.10 AC-12 Session Termination

Contractors, including those using a CSP, must automatically terminate a user session (application session) after 30 minutes of inactivity.

Session termination addresses the termination of a user session (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions.

13.11 AC-14 Permitted Actions without Identification or Authentication

Contractors, including those using a CSP, must identify and document specific user actions that can be performed on the information system without identification or authentication and permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives. Examples of access without identification and authentication would be instances in which the contractor maintains a publicly accessible web site allowing users to access information on the site, without providing valid identification and authentication information.

13.12 AC-17 Remote Access

Contractors, including those using a CSP, must document usage restrictions, configuration/connection requirements, implementation guidance, and authorize each type of remote access to the information system prior to allowing connections.

Contractors, including those using a CSP, must employ automated mechanisms to monitor and control remote access methods. Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, laptop computers, workstations, smartphones, and tablets.

Anytime a contractor or CSP allows an employee or IT support personnel to remotely access the contractor's IT environment that houses and/or processes IRS SBU data, the connection must be secured using a Virtual Private Network (VPN) using Two-factor Authentication (2FA) and FIPS 140-2 or later validated encryption modules. 2FA requires the use of 1) something they know, (such as a password) and 2) something they possess, (such as a token card), to access the information system.

The information system must route all remote access through a limited number of managed access control points. Remote Access to contractor IT environments that support the IRS contract utilizing IRS issued laptops/equipment or contractor owned/operated laptops/equipment is forbidden from locations outside the US and its territories.

Contractors using a CSP must ensure that the CSP provides the capability to disconnect or disable remote access to the information system within 15 minutes.

Supplemental C-SCRM Guidance: Supply chains are typically accessed remotely. Whether for the purpose of development, maintenance, or the operation of information systems, contractors must implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to a contractor's supply chain (including distributed software development environments) must be limited to the contractor or contractor personnel and only if and as required to perform their tasks. Remote access requirements must be properly defined in agreements. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.13 AC-18 Wireless Access

The Contractor must authorize, document, and monitor all wireless access to the information system. Contractors must create and maintain documentation that defines wireless configurations and restrictions. Only users identified and explicitly authorized must be allowed to configure wireless networking capabilities.

Contractors, including those using a CSP must protect wireless access to the information system using authentication of users and devices, and require FIPS 140-2 or later validated encryption modules. This includes contractor personnel utilizing personally provided wireless capabilities to access contractor systems remotely from home and alternative work locations.

Contractors, including those using a CSP, must disable, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. Unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, and other devices must be disabled and monitored for unauthorized changes.

13.14 AC-19 Access Control for Mobile Devices

A procedure must be developed to authorize, document, and monitor mobile device access to the contractor's information system. Information must be sufficient to enable all activities to be logged.

Contractors, including those using a CSP, must develop policies for allowed portable and mobile devices, for information systems that contain SBU data. This includes the use of smartphones, tablets, etc. The policies must document the approved or disapproved use of mobile devices to connect to IT assets that house IRS SBU.

IRS issued laptops/mobile devices or contractor laptops/mobile devices containing IRS SBU data must not be taken outside of the United States or its territories.

Electronic, optical, and other removable media must be kept in a secured area under the immediate protection and control of authorized contractor personnel or locked up. When not in use, the media must be promptly returned to a proper storage area/container. For more information, please see Section 22.0 Media Protection.

IRS SBU data may be stored on mobile devices only if contractor-approved security access control devices (hardware/software) have been installed and are receiving regularly scheduled maintenance and security patches.

All mobile computing devices must employ full-disk encryption. This includes but is not limited to desktop/laptop computers, Compact Disk (CD), Digital Video Device (DVD) media, thumb drives, or any media that can be used to house IRS SBU data that can be easily transported by an individual. IRS SBU that resides on removable media must be encrypted with FIPS 140-2 or later validated encryption modules.
Contractors supporting or allowing personally owned devices, also known as Bring Your Own Device (BYOD) to store, process, or access IRS SBU data must:

- Register all BYOD devices with the company and manage them via a Mobile Device Manager (MDM) server.
- Consent to remote inspection and monitoring of the approved mobile access solution on their approved personally owned mobile device.
- Ensure they are the only person who has access to their approved personally owned mobile devices when being used to view or process IRS SBU information.
- Ensure a valid password is successfully entered prior to logging onto the mobile device.
- Only approved personally owned mobile devices must be permitted to process or store IRS SBU, including IRS email.
- The device must have sandboxing capability to segment company and/or IRS SBU data from the employees' personal information.
- The MDM must have the ability to remotely erase the sand box when the BYOD device is lost, stolen, or the employee is no longer working for the company.
- The Sandbox partition must be encrypted utilizing FIPS 140-2 or later validated encryption modules.

- Applications stored on the corporate sandbox partition must be approved and distributed by the company via the MDM.
- Employees' personal apps must not be able to communicate with containerized apps, nor can data be copied and pasted from a containerized app to a non-containerized application.
- BYOD users must not use administrative accounts for general tasks, such as reading email, web browsing, and social networking, because such tasks are common ways of infecting devices with malware.
- The device must include antivirus and anti-malware software with the capability to receive updates automatically. The software must be configured to scan in real-time and perform full system scans at least weekly.
- The transfer of files via instant messaging platforms must be restricted. If the software can transfer files with other instant messaging users, it should be configured to prompt the user before permitting a file transfer to begin.
- Jailbreaking or installing a rootkit on BYOD devices is strictly prohibited. Doing so disables the manufacturer's built-in security capabilities for the device.
- The use of public WIFI hotspots is prohibited unless the device is connected via a contractor approved VPN connection that utilizes FIPS 140-2 or later validated encryption modules.
- A firewall must be installed and active on all mobile devices.
- BYOD participants must not store any IRS SBU data on a removable media.
- IRS SBU must not be viewed or discussed on mobile devices in public places (e.g., airports, coffee shops, hospitals, malls, etc.), and
- MDM servers must be configured to detect rooted or jailbroken devices.

Contractors using a CSP must ensure that the CSP employs either full-device encryption or container encryption to protect the confidentiality and integrity of information on all mobile devices.

13.15 AC-20 Use of External Systems

External systems are information systems or components of systems, that are outside of the authorization boundary established by the organization and for which the organization has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

Contractors, including those using a CSP, must ensure that only those IT assets identified for processing of IRS SBU must be used to support the IRS contract. IT assets not identified to the IRS as being in the scope of IRS contract are considered external information systems. The contractor and subcontractor must not use other external information systems within their home or business for the purpose of conducting IRS work.

If external information systems are required, trust relationships must be established both logically and in writing and external components must be identified to the IRS.

Contractors, including those using a CSP, must permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

- Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan, and
- Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. The contractor must limit the use of organization-controlled portable storage devices media by authorized individuals on external information systems.

Contractors, including those using a CSP must ensure that they, or the CSP must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- Access the information system from external information systems, and
- Process, store, or transmit IRS SBU using external information systems.

Contractors, including those using a CSP must ensure that they, or the CSP must restrict the use of Contractor or CSP-controlled portable storage devices by authorized individuals on external information systems.

Supplemental C-SCRM Guidance: Contractors' external information systems include those of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Unlike in an acquirer's internal Contractor where direct and continuous monitoring is possible, in the external supplier relationship, information may be shared on an as-needed basis and should be articulated in an agreement. Access to the supply chain from such external information systems must be monitored and audited. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

13.16 AC-21 Information Sharing

Contractors, including those using a CSP must ensure that they facilitate information sharing, as allowed by the IRS or contract. This can be done by identifying the appropriate personnel who review and authorize sharing, to determine if the information being shared with a partner organization matches the contractor access requirements for the information being shared.

Contractors, including those using a CSP must employ automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

This requirement applies to information that may be restricted in some manner (e.g., contract-sensitive information, proprietary information, PII, IRS SBU data based on some formal or administrative determination). Depending on the information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

13.17 AC-22 Publicly Accessible Content

Contractors, including those using a CSP must; ensure that they designate, and train personnel authorized to post information onto a publicly accessible information system as allowed by the IRS or contract.

13.18 AC-23 Data Mining Protection – C-SCRM Control

The Contractor must employ data mining prevention and detection techniques to detect and protect against unauthorized data mining.

Supplemental C-SCRM Guidance: Contractors must implement this control as part of their insider threat activities and flow down this requirement to relevant sub-tier contractors.

14.0 Awareness & Training (AT)

The IRS has established policies and procedures to ensure Awareness Training takes place at contractor sites.

14.1 AT-1 Awareness & Training Policy and Procedure

Contractors, including those using a CSP, must designate an official to manage the development, documentation, and dissemination of the AT policies and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Contractors, including those using a CSP, must review/update AT policies and procedures annually, or if there is a significant change to awareness and training policies or procedures.

14.2 AT-2 Security Awareness Training

Contractors must ensure all contractor personnel who require access to IRS SBU data or information systems complete the IRS required Security Awareness Training (SAT). This applies to contractors working at contractor-managed facilities using contractor-managed IT assets.

IRS SAT is a combination of IRS mandatory briefings that include:

- IRS Annual Cybersecurity Awareness
- Privacy, Information Protection, & Disclosure (PIPD)
- Records Management Awareness
- Insider Threat Awareness
- FMSS Physical Security
- IRS CUI General Awareness
- UNAX Awareness

For each contractor employee assigned to a contract/order that is not connected to the IRS infrastructure, the contractor must submit confirmation of completed SAT to the COR.

Contractors who have access to the IRS network must complete SAT via the IRS online training system Integrated Talent Management (ITM). For contractors that don't have access to the IRS network the COR will provide training materials to the contractor.

IRS SAT must be completed by contractor personnel within 5 business days of being granted interim/final staff-like access as outlined in the contract requirements language entitled "Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access" and before being granted access to IRS SBU data. Thereafter, contractor personnel assigned to the contract/order must complete IRS SAT annually by October 31. The date listed on the memorandum provided by IRS Personnel Security must be used as the commencement date of staff like access.

It is the responsibility of the contractor to ensure all briefing materials have been received and distributed to contractor and subcontractor employees. This includes all contractor personnel who provide support to the IRS contract, who are located remotely or on-site. The contractor is responsible for providing the list of all employees who have completed training to the IRS COR.

14.3 AT-3 Role Based Training

Contractor personnel who have a significant IT role/responsibility must complete 8 hours of Specialized IT security (SITS) training. Significant IT roles are defined in the table below.

Significant IT Roles
Chief Information Security Officer (CISO) - Individual responsible for the security of an entire organization.
Authorizing Official (AO) - Individual with the responsibility to authorize the use of an information system.
Information System Security Officer (ISSO) - Individual with the responsibility for the security of an information system.
Information System Security Manager (ISSM) - Oversees the cybersecurity program for an information system.
Cybersecurity Policy and Guidance Personnel - Individuals responsible for developing and/ or maintaining cybersecurity policy and procedure.
Incident Analyst/Handler/Responder/Investigator - Individuals responsible for providing security operations center services to an organization.
Network Administrator - Individuals with the responsibility of oversight and management of a network, including implementation of security requirements.
System Administrator (SA) - Individuals with the responsibility of oversight and management of a system, including implementation of security requirements.

Database Administrator (DBA) - Individuals with the responsibility of oversight and management of a database, including implementation of security requirements.
System Programmer/Developer - Individuals with the responsibility to develop or modify software code.
Quality Assurance Personnel - Individuals responsible for ensuring the quality of an information system and/ or it's data.
Change Management Personnel - Individuals with change management (patching, configuration changes, functionality changes, etc.,) responsibilities.
Help Desk/IT Services Personnel - Individuals part of the Help Desk or IT Services staff.

There are various sources for SITS training including ITM, contractor learning systems, and free web-based training available to government contractors. IT security training completed by contractors within the last year as part of continuing education may be accepted at the discretion of the CSA team. Evidence for SITS training must include name of course, attendee name, date completed, length of course. As a convivence to contractors a website where free SITS training is available @ https://niccs.cisa.gov/education-training/cisa-learning

Contractor personnel newly assigned to a significant IT role, including at time of contract award, must complete SITS Training prior to being granted access to IRS SBU. Annually thereafter, contractor personnel assigned to the IRS contract/order must complete SITS annually by June 1st of each calendar year.

Existing contracts that have been modified or will be modified to include contractor and subcontractor personnel identified as having a significant IT role must complete the SITS Training within 45 days of the contract modification designating an employee to a significant IT role and annually by June 1st, thereafter.

Supplemental C-SCRM Guidance: Contractors must designate an official to manage the development, documentation, and dissemination of the training policy and procedures, including C-SCRM and role-based specific training for those with supply chain responsibilities. Contractors must integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the contractor and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response.

14.4 AT-4 Training Records

Contractors who have access to the IRS learning system, (ITM) must ensure that all contractor's training is completed and recorded in ITM. Contractors who have do not have

access to ITM must send training records to the IRS COR who is responsible for uploading them to ITM. ITM is the system of record for IRS training records.

15.0 Audit and Accountability (AU)

Contractors, including those using a CSP, must ensure that, where more than one employee is allowed to access an IT asset, including servers, workstations, laptops, storage arrays, and cloud computing services etc., the Contractor must enable auditing on those assets to ensure that actions are logged, and access to IRS information will be deterred, detected, monitored, and tracked. Audit records must not include any PII information that is not necessary to identify the event.

15.1 AU-1 Audit and Accountability Policy and Procedures

Contractors, including those using a CSP, must designate an official to manage the development, documentation, and dissemination of the AU policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Contractors, including those using a CSP, must review/update AU policies and procedures annually. The policies and procedures must be sufficient to enable monitoring of IT assets.

15.2 AU-2 Event Logging

Contractors, including those using a CSP, in support of the IRS contract, must implement event logging to record and monitor access to IT assets, including, but not limited to routers, operating systems, databases, remote access, file access, and applications.

Contractors, including those using a CSP must identify and enable logging events that allow the contractor to detect, deter, and report on suspicious activities. The required logging events are listed in the tables below.

Table 2: System Logging Events

Successful and Unsuccessful Logon attempts
Account Logon/Logoff Events
Account Management Events

Object Access
Policy Change
Privileged functions
Process Tracking
System Events
Web Application Events
All administrator activity
Authentication checks
Authorization checks
Data deletions
Data access
Data changes
Permission changes

Contractors, including those using a CSP, and/or using including Commercial Off-the-Shelf (COTS) solutions to store, process, and collect FTI must retain event logs to support audit analysis and investigations of unauthorized access. The system must record and retain the following information in a data transaction or event log; the user's identity, date, and time of access to FTI, action taken, and which account was accessed.

Contractors shall configure call recording systems to capture and retain call recording meta-data and have the capability to search the meta-data for the purposes of play-back, quality assurance, and a record of file access.

Meta-data associated with the voice recording must include the following information:

- The staff member initiating or receiving the call,
- The data, time, and duration of the conversation,
- A way to track the identity of the taxpayer, and
- Access to the voice recording (to identify UNAX violations).

Supplemental C-SCRM Guidance: An observable occurrence within the information system or supply chain network must be identified as a supply chain auditable event based on the Contractor's System Development Lifecycle (SDLC) context and requirements.

Auditable events may include software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems.

Contractors must incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Contractors and subcontractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

15.3 AU-3 Content of Audit Records

The Contractor must configure the information system to generate audit records containing enough detail to facilitate the reconstruction of events. Events may include unauthorized activity, a system malfunction, or tampering is suspected in the audit records, for audit events identified by type, location, or subject.

Examples of content that may satisfy this requirement are time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Contractors, including those using a CSP must generate audit records containing information that establishes:

- What type of event occurred,
- When the event occurred,
- Where the event occurred,
- The source of the event,
- The outcome of the event, and
- The identity of any individuals, subjects, or objects/entities associated with the event.

Contractors, including those using a CSP must consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal PII in the audit records, especially if the records inputs or is based on patterns or time of usage.

Contractors, including those using a CSP must limit PII in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system. Contractors must limit IRS PII contained in their audit records to only collecting the approved IRS PII data elements as listed in the PCLIA.

Supplemental C-SCRM Guidance: The audit records of a supply chain event should be securely handled and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information

and its sources as appropriate. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

15.4 AU-4 Audit Log Storage Capacity

Contractors, including those using a CSP, must allocate storage capacity to accommodate audit log retention requirements. Audit log retention must be sufficient to enable log management and retrieval of auditable events as necessary. Log storage capacity must be defined in the system security documentation.

15.5 AU-5 Response to Audit Logging Processing Failures

Contractors, or CSPs must develop and implement an action plan that can be used in an audit processing failure.

If the audit system becomes full and/or audit log generation malfunctions, the information system must be configured to alert contractor or CSP personnel in real-time to take action to ensure audit records are retained and audit log generation is restored. Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity.

15.6 AU-6 Audit Record Review, Analysis, and Reporting

Automated reports must be generated and designated personnel must review reports to identify unusual activity and act if necessary. Contractors, including those using CSP's, must document the timeframe for conducting reviews of audit information in their audit policy or procedure.

Contractors, including those using a CSP, must employ automated mechanisms to integrate audit review, analysis, and reporting processes to support contractor processes for investigation and response to suspicious activities.

Automated audit reports/records must be generated, analyzed, and correlated across different repositories to gain contractor/CSP-wide situational awareness.

Integrated analysis requires that the information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information.

Audit record review, analysis, and reporting covers information security and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP).

All compromises to IRS SBU data are required to be identified as an information security incident, and reported to the IRS CSIRC Incident Response Operations Team, at (240) 613-3606**.** See procedures in Section 20.0, Incident Response for further instructions.

Contractors using a CSP must ensure that they, or the CSP will review and analyze information system audit records at least weekly; for indications of inappropriate or unusual activity.

15.7 AU-7 Audit Record Reduction and Report Generation

Audit record reduction and report generation on contractor, or CSP information systems must provide capabilities that support on-demand audit review, analysis, reporting requirements, and after-the-fact investigations of security incidents. This capability must not alter the original audit log content records.

The information system must provide the capability to automatically process audit records and search for events of interest based on selectable event criteria.

15.8 AU-8 Time Stamps

All audit records generated on contractor, or CSP information systems must contain a timestamp. Internal system clocks must generate the timestamp for audit records. Information systems must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC), or Greenwich Mean Time (GMT) and meets one second granularity of time measurement.

Contractors, including those using CSP's must compare internal information system clocks with an authorized enterprise-wide time source and synchronize the internal system clocks to the authoritative time source when the time difference is greater than one second.

15.9 AU-9 Protection of Audit Information

Contractors, including those using CSP, must define all individuals who are responsible for reviewing audit information upon detection of unauthorized access, modification, or deletion. Access must be restricted so that only authorized personnel have access to audit information. The management and retention of all audit information must remain in control of the contractor identified in the IRS contract and safeguarded as SBU data. Audit logs must be protected by access controls to prevent unauthorized access to ensure events are not modified or deleted.

Audit records must be stored at least weekly in a repository that is part of a physically different system or system component than the system or component being audited. Cryptographic mechanisms must be implemented to protect the integrity of audit information and audit tools.

15.10 AU-11 Audit Record Retention

The Contractor must retain audit records for seven years if the contractor is processing/storing/or transmitting FTI. Otherwise, audit records must be retained for three years for the purpose of providing support in after-the-fact investigations of security incidents. Copies of audit records must be provided to the IRS when requested to investigate potential IRS security events.

The Contractor must send questions regarding IRS record retention requirements to the COR, who will forward them to PGLD.

Contractors using a CSP must ensure that audit records are retained online for a minimum of 90 days to provide support for after-the-fact investigations of security incidents and preserve audit records offline in accordance with IRS record retention requirements.

15.11 AU-12 Audit Record Generation

Auditing tools must be in place to allow contractors, including those using CSP's to generate reports to enable a review of audit events based on contractor needs. For example, if file directories have restricted access, the audit must log all accesses to that directory.

The information system must have the capability to allow the selection of auditable events for specific information system components.

Contractors using a CSP, must ensure audit tools must collect audit records from all networks, data storage, and computing devices into a system-wide (logical or physical) audit trail.

Supplemental C-SCRM Guidance: Contractors must ensure that audit record generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include component version updates, component approvals from acceptance testing results, logistics data-capturing inventory, or transportation information. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

15.12 AU-13 Monitoring for Information Disclosure (C-SCRM Control)

Contractors must monitor social networking sites (e.g., Facebook, X, Instagram,) and Open-Source information code sharing platforms (e.g., GitHub) for evidence of unauthorized disclosure of contractor information.

If an information disclosure is discovered, the Contractor must notify the IRS COR immediately upon discovery and take actions to have the unauthorized information removed and identify the source of the unauthorized disclosure.

15.13 AU-14 Session Audit (C-SCRM Control)

Contractors must provide the SA, or SAs the capability to record, view, and/or log the content of a user session as part of an investigation.

Session auditing activities must be developed, integrated, and used in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

15.14 AU-16 Cross Organization Audit Logging | Sharing of Audit Information (C-SCRM Control)

Contractors must identify, through an organizational sharing agreement, cross-organizational audit information sharing requirements.

16.0 Assessment, Authorization, and Monitoring (CA)

An assessment of controls provides the Contractor and IRS with an assurance that security and privacy controls are established and operating, as intended, within the contractor environment. Key points of the CA process include:

- Conducting an independent assessment to ensure the contractor-defined security and privacy controls are operating as intended.
- Identification of weaknesses/risks.
- Briefing management of weaknesses/risks.
- Formal IRS acceptance of any associated risks or mitigation of risks or implementation of compensating controls, and
- Accrediting the environment by authorizing the environment to be operational, by a contractor official.

Assurances must be made to ensure security and privacy controls have been applied; that testing has been conducted to validate controls; and that a contractor official has authorized the use of the IT assets, and identified any risks accepted by the contractor.

16.1 CA-1 Assessment, Authorization, and Monitoring Policies and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the CA policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Contractors, including those using CSP's must review/update CA policies and procedures annually, and immediately after security or privacy incidents or a breach.

16.2 CA-2 Control Assessments

Contractors, including those using CSP's must develop a security and privacy control assessment plan and produce a security and privacy control assessment report with the results of the assessment. The CA plans are required to be reviewed and signed by the Privacy Official or Authorizing Official prior to conducting the assessment.

Contractors, including those using CSP's must conduct control assessments annually, or when major changes have been made to the IT and privacy environments to ensure the security and privacy controls are implemented correctly, operating as intended, and meeting security and privacy requirements.

When the testing of a security control reveals that the control is not functioning as expected and corrective action has been taken to mitigate the weakness, the finding and corrective action must be documented within the testing documentation.

The results of security and privacy control assessments must be documented in a control assessment report and provided to the CSA Team upon request.

16.3 CA-3 Information Exchange

Contractors must maintain a list that defines the external systems in use that support the IRS contract.

Contractors, including those using CSP's, must authorize connections from their information system to other information systems using an Interconnection Security Agreement (ISA).

For each system interconnection the contractor, or CSP must document the interface characteristics, security and privacy requirements, controls, and responsibilities for each system.

ISAs must be reviewed annually and updated when necessary.

The Contractor, based on a risk assessment, must employ a deny-all, permit-by-exception policy for allowing contractor IT assets to connect to external information systems.

The Contractor must configure all equipment connected to the contractor system or network where IRS data is being processed or stored, to meet IRS Publication 4812 security and privacy requirements.

This control applies to dedicated connections between the information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing, or to connections with external providers who are only providing telecommunications and transmission services.

Supplemental C-SCRM Guidance: The exchange of information or data between the information system and other systems requires scrutiny from a supply chain perspective. This includes understanding the interface characteristics and connections of those components/systems that are directly interconnected or the data that is shared through those components/systems with developers, system integrators, external system service providers, other ICT/OT-related service providers, and – in some cases – suppliers.

Proper Service-Level Agreements (SLA) must be in place to ensure compliance to system information exchange requirements defined by the contractor/subcontractor, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies.

Examples of such interconnections can include:

- A shared development and operational environment between the contractor and system integrator.
- Product update/patch management connection to an off-the-shelf supplier, and
- Data request and retrieval transactions in a processing system that resides on an external service provider shared environment.

Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

16.4 CA-5 Plan of Action and Milestones (POA&M)

For security or privacy reports issued to the contractor including CSAs and continuous monitoring activities, the contractor is responsible for developing a POA&M. The POA&M must identify corrective actions for any identified findings.

When a CSA initial report is issued to the COR, the contractor must create and provide an initial POA&M and remediation evidence to the COR and CSA Team @ IT.Cyber.CSA.POAM@irs.gov within business 30 days. Thereafter, the contractor must provide an updated POA&M and remediation evidence (or POA&M Status update if not corrected) monthly to the COR and CSA Team @ IT.Cyber.CSA.POAM@irs.gov demonstrating progress made toward remediation, until all findings are determined to be tentatively closed by the CSA Team.

16.5 CA-6 Authorization

Contractors, including those using CSP's must designate a senior official as the Authorizing Official for the information system. The assigned senior official must authorize the information system prior to it being put into operation, document the authorization, and sign the documentation as the responsible party. By authorizing an information system to operate, the senior official is accepting the risk for the information system. The senior official must ensure the information systems authorization is reviewed and updated every three years, or when a significant impact to the information system occurs.

At a minimum, the final authorization packages must consist of the following deliverables:

- Security and Privacy Plans
- Security and Privacy Assessment Reports
- Privacy and Civil Liberties Impact Assessment (PCLIA),
- Active POA&Ms,
- Executive Summary
- Auditing Plan, and
- Authorization Decision Document must include:
    - Authorizing Decision,
    - Terms and Conditions for the Authorization,
    - Authorization Termination Date, and
    - Executive Summary of Risk.

16.6 CA-7 Continuous Monitoring

Contractors, including those using CSP's must establish and implement a continuous monitoring strategy that includes a configuration management process, a security and privacy impact analysis of changes to an information system, and continuous/ongoing security and privacy control assessments.

The Contractor or CSP must implement a continuous monitoring strategy that includes active and ongoing monitoring of the security controls (e.g., monthly configuration scans and vulnerability scans) and privacy controls, in accordance with the defined configurations to identify any controls that may not be compliant. The Contractor and subcontractor must report the security and privacy status of the system to the Contractor Security Representative (CSR).

The Contractor or CSP must ensure risk monitoring is an integral part of the continuous monitoring strategy, including:

- Effectiveness monitoring,
- Compliance monitoring, and
- Change monitoring.

Contractors using a CSP must ensure that the CSP conducts Operating System (OS) scans, database scans, and web application scans at least monthly. An independent assessor must conduct a complete scan of OS, databases, and web applications at least annually.

16.7 CA-8 Penetration Testing

The Contractor must conduct penetration testing using an independent team when an information system is put into production and at a minimum every three years thereafter using risk assessment results to establish testing prioritization.

Contractors using a CSP, must ensure that the CSP will conduct penetration testing using an independent penetration agent or team at least annually on all information systems.

16.8 CA-9 Internal System Connections

Contractors and subcontractors, including those using CSP's must authorize any internal connections to IT assets processing IRS SBU data and document the interconnection characteristics, security and privacy requirements, and the type of information being transmitted between IRS assets and any other internal contractor information systems. The contractor must review connections annually to ensure connections are still needed.

17.0 Configuration Management (CM)

CM ensures that organizations are using the correct versions of configurations, settings, and baselines, and that there are formal mechanisms in place to implement new configurations, settings, and baselines.

17.1 CM-1 Configuration Management Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the CM policy and procedures. Security and privacy programs must collaborate on the development of the CM policy and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor or CSP must review/update CM policies and procedures annually, or if there is a significant change to ensure adequate CM policy and procedures are developed and implemented.

17.2 CM-2 Baseline Configuration

Contractors, including those using CSP's must develop, document, and maintain a current baseline configuration for all IT assets. This inventory must include all databases, applications, operating systems etc. that are being used as part of the baseline configuration for servers, routers, workstations, etc.

- The Contractor or CSP must review and update the baseline configuration of the information system; annually, when there is a significant change, as an integral part of information system component installations and upgrades.
- The Contractor or CSP must retain at least one previous version of the baseline configuration to support rollback. The Contractor or CSP must use automated mechanisms to retain the current configuration baselines. Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools.
- The Contractor or CSP must maintain a baseline configuration for system development and test environments that is managed separately from the production baseline configuration.

Supplemental C-SCRM Guidance: Contractors must establish a baseline configuration of both the production information system and the development environment, including documenting, formally reviewing, and securing the agreement of stakeholders. The purpose of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance.

The baseline configuration must take into consideration the Contractor's production environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with the organization's information systems and networks.

If the system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

17.3 CM-3 Configuration Change Control

Contractors, including those using CSP's must develop and implement a configuration change control process. This process must include a formal written change request to be submitted to the appropriate Change Control Board (CCB) for all changes, scheduled and unscheduled. The CCB must include information security and privacy representatives. This process must ensure that all changes are approved, tested, documented, and published; using a change control log that is available for review. This log must be retained using automated tools, such as: change management software, spreadsheets, databases, etc.

Development and testing environments must be physically and/or logically separated from production environments.

Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, vulnerability remediation and unscheduled or unauthorized changes. For changes that impact privacy risk, the contractor's representative for privacy must update privacy impact assessments.

Change logs must be retained for three years as confirmed by the IRS Records and Information Management (RIM) Office. The Contractor must test, validate, and document changes to the test information system before implementing the changes on the production information system.

Supplemental C-SCRM Guidance: Contractors must determine, implement, monitor, and audit configuration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for C-SCRM. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

17.4 CM-4 Impact Analysis

Contractors, including those using CSP's must ensure changes to information systems are analyzed in a test environment prior to implementation into the production environment as part of the change approval process to determine potential security and privacy impacts.

Impact analysis may include, reviewing security and privacy plans to understand control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security and privacy impact analysis may also include assessments of risk to better understand the impact of the changes and to determine if additional security or privacy controls are required.

If potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks, then the contractor must notify and work with the COR to update the contract PCLIA.

17.5 CM-5 Access Restrictions for Change

Contractors, including those using CSP's must:

- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- Limit privileges to change information system components and system-related information within a production environment; and review and reevaluate privileges at least quarterly.
- Take measures to protect devices against the bypass of software controls arising from booting from any sources other than those designated by the SA for such purposes.

17.6 CM-6 Configuration Settings

Contractors, including those using CSP's must establish and document configuration settings for information technology products employed within the information system using security configuration tools. Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. The contractor must run compliance scans on the information system at least monthly.

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluations. The specifications comprising SCAP include Extensible Markup Language (XML) and enumerations. Working in conjunction, vulnerability and compliance information can be shared and executed between any SCAP enabled products. Vulnerability and policy content created using SCAP can be used with vulnerability scanning products to perform vulnerability management, measurement, and policy compliance evaluations.

Any deviations from established configuration settings for information system components must be identified, documented, and approved based on operational requirements. Changes to the configuration settings must be monitored and controlled in accordance with defined configuration change management policies and procedures.

Contractors, including those using CSP's must document all deviations from the standard security controls and ensure these are brought into compliance using a standard configuration process.

Contractors using a CSP must ensure that they or the CSP verify that the configuration settings are established and documented for information technology products employed within the information system using United States Government Configuration Baseline (USGCB).

- If USGCB is not available, the service provider must use the Center for Internet Security (CIS) guidelines (Level 1) to establish configuration settings.

Supplemental C-SCRM Guidance: Contractors must oversee the function of modifying configuration settings for their information systems and networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in the creation of contractor information systems and networks on a need-to-know basis. Changes must be tested and approved before they are implemented. Configuration settings must be monitored and audited to alert designated Contractor personnel when a change has occurred. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

17.7 CM-7 Least Functionality

All IT assets must be configured to ensure that least functionality is implemented to restrict the information system to only essential ports, protocols, software, and services. Protocols, services, and logical ports that must be restricted, include but are not limited to: FTP, Telnet, SQL services enabled on non-SQL servers, and USB ports. The contractor must ensure compliance with all defined requirements related to functions, ports, protocols, and services.

Contractors, including those using a CSP, must identify all programs authorized or prohibited to be used in the IT environment, and define policies, rules of behavior, and/or access agreements regarding software program usage and restrictions.

The Contractor, or CSP must review the information system at least annually and during transition periods from older technologies to newer technologies to identify and disable unnecessary functions, ports, protocols, software, and/or services.

The information system must prevent unauthorized software from being executed.
The Contractor, or CSP must identify all software authorized to be used on the information system. A "deny-all, allow-by-exception" policy must be employed to prohibit the execution of unauthorized programs.

The list of authorized software must be reviewed and updated annually. By default, the Contractor must maintain the most restrictive permissions and usage of programs.

The Contractor must scan their networks, at minimum annually, to detect and remove any unauthorized or unlicensed software.

Contractors using a CSP must ensure that they or the CSP configure the information system to provide only essential capabilities. The service provider must use the CIS guidelines to establish a list of prohibited or restricted functions, ports, protocols, and/or services; or establish its own list of prohibited or restricted functions, ports, protocols. The information system must prevent program execution using a list of authorized software programs (i.e., whitelist. The CSP must review and update the list of authorized software programs at least annually.

Supplemental C-SCRM Guidance: Contractors must select components that allow the flexibility to specify and implement least functionality. Contractors must ensure least functionality in their information systems and networks and throughout the SDLC. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

17.8 CM-8 System Component Inventory

Contractors including those using CSP's must develop and maintain an inventory of all hardware, software, removable media, components, and a software whitelist/blacklist for the information system that supports the IRS contract. The inventory must include: an inventory serial number, description of the inventory item, owner of the inventory item, date placed in inventory, and date inventory was validated. The inventory must not include duplicate accounting of components or components assigned to any other system. The inventory must be reviewed and reconciled annually. The inventory must be sufficient to enable recovery of IT assets that are identified as lost, stolen, or disclosed. The contractor or CSP must update the inventory of information system components as an integral part of component installations, removals, and information system updates.

The Contractor or CSP must employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system and must take the following action when unauthorized components are detected:

- Disable network access by such components,
- Isolate the components, and
- If elevated to an incident the COR must be notified immediately upon discovery.

Supplemental C-SCRM Guidance: Contractors must ensure that critical component assets within the information systems and networks are included in the asset inventory. The inventory must also include information for critical component accountability. Inventory information includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and – for networked components

or devices – machine names and network addresses. Inventory specifications may include the manufacturer, device type, model, serial number, and physical location. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Contractors must specify the requirements and how information flow is enforced to ensure that only the required information - and no more - is communicated to the various participants in the supply chain. If information is collected and parsed downstream, there should be information about who created the subset information. Contractors must consider producing Software Bill of Materials (SBOM) for applicable and appropriate classes of software, including purchased software, open-source software, and in-house software.

17.9 CM-9 Configuration Management Plan

Contractors including those using CSP's must develop, document, and implement a CM plan for the information system that addresses roles, responsibilities, and CM processes and procedures. A process must be established for identifying configuration items throughout the SDLC and for managing the configuration of the configuration items. Configuration items for the information system must be defined and configuration items must be placed under CM. The CM plan must be reviewed annually and signed by contractor or CSP designated personnel and protected from unauthorized disclosure and modification.

Supplemental C-SCRM Guidance: Contractors must ensure that C-SCRM is incorporated into CM planning activities. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

17.10 CM-10 Software Usage Restrictions

Contractors including those using CSP's must use software and associated documentation in accordance with contract/order/agreement and copyright laws. The contractor or CSP must track the number of software licenses.

Contractors including those using CSP's must establish the following restrictions on the use of open-source software:

a. A security assessment is conducted prior to deploying.
b. A software support plan is developed.
c. The Open-Source Software license permits modification for internal use without being obligated to distribute the source code to the public.
d. Updates to Open-Source Software including code fixes and enhancements, developed for the IRS contract must not be released to the public.

17.11 CM-11 User-Installed Software

Contractors, including those using CSP's must establish policies governing the installation of software by users.

Contractors, including those using CSP's must enforce software installation policies through the following methods:

i. Procedural methods (e.g., periodic examination of user accounts);
ii. Automated methods (e.g., configuration settings implemented on organizational systems); and
iii. Continuously monitor policy compliance.

To maintain control over the types of software installed, organizations must identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious.

17.12 CM-12 Information Location

Contractors including those using CSP's must identify and document:

- The location of IRS SBU data and the specific system components on which the information is processed and stored, and
- The users who have access to the system and system components where the information is processed and stored.

Contractors including those using CSP's must utilize automated information location tools to manage the data produced during information location activities and share information across the organization. Changes to the location where the information is processed and stored must be tracked and documented.

18.0 Contingency Planning (CP)

Contractors, including those using CSP's must develop a CP and business resumption plan to provide information for how the contractor, subcontractor, or CSP must restore business operations and resume business in the event of failed IT assets or the inability to access the facility.

18.1 CP-1 Contingency Planning Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the CP policy and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Contractors, including those using CSP's must review/update CP policies and procedures annually, or if there is a significant change that defines company requirements in terms of IT CP or following certain events including: assessment or audit findings, and security or privacy incidents.

The contingency plan must be updated to address changes to the organization, system, or environment of operation, and problems encountered during contingency plan implementation, execution, or testing. Lessons learned from contingency plan testing, training, or actual contingency activities must be incorporated into contingency testing and training.

The policies and procedures must be sufficient to address the planning elements required for a contractor, subcontractor, or CSP environment. Policies and procedures must address the need to identify essential business functions supported, provide restoration priorities, and identify contingency roles and responsibilities.

Disaster recovery plans must be developed, tested, and maintained for mission or business critical systems for use if normal operations cease.

18.2 CP-2 Contingency Plan

Contractors, including those using CSP's must develop a contingency plan to address IT and physical security planning. Contingency plans must identify key business functions provided to the IRS, alternate work sites, alternate resources, contact information, and define the

Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The plans must document the activities associated with restoring all IT assets, including information systems and applications after a disruption or failure. The Contingency Plan must be reviewed/updated at least annually.

For Contractors with contracts that support IRS Filing Season systems/processes and/or IRS Mission Essential Functions (MEFs), the RPO and RTO defined in the contractor/subcontractor CP must be the same as the RPO and RTO defined in the IRS MEF's CP. The RPO and RTO for IRS Filing Season systems/processes and/or IRS MEFs must be obtained from the COR. Where applicable, when a contractor supports a MEF system, the Maximum Tolerable Downtime of 12-hours end-to-end must be considered in the disaster recovery plans and cloud computing requirements.

As part of CP, an Occupant Emergency Plan (OEP) must be included to address occupant safety and security procedures, in the event of an emergency. The OEP should be shared with all employees who have work related to the IRS contract or any impacted employees. At least annually, the plan must be reviewed, updated, with OEP drills being conducted. The results must be documented, and lessons learned incorporated into the OEP.

Contractors, including those using CSP's must distribute copies of the CP to key personnel who are responsible for implementing and ensuring updates are communicated. A copy of the CP must be provided annually to the COR.

The CP is considered SBU data and must be protected from unauthorized disclosure and modification.

Contractors, including those using CSP's must coordinate CP development with contractor groups responsible for related plans. Related plans include Business Continuity Plans (BCP), Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and OEP.

18.2.1 CP-2(7) Contingency Plan | Coordinate with External Service Providers (C-SCRM Control)

Contractors must coordinate their CP with the CPs of their external service providers to ensure that contingency requirements can be satisfied.

18.3 CP-3 Contingency Training

Contractors, including those using CSP's must train personnel in their contingency roles and responsibilities within 30 days of assuming a contingency role or responsibility, when changes to the information system are sufficient to warrant the training, and to provide refresher training annually.

Training content must be reviewed and updated annually, when there are major system changes, or following certain events including: CP testing, security or privacy assessments, audit findings, and security or privacy incidents.

Supplemental C-SCRM Guidance: Contractors must ensure that critical suppliers are included in contingency training. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

18.4 CP-4 Contingency Plan Testing

Contractors, including those using CSP's must develop and test a CP to ensure that operations can be restored. CPs must be tested annually, the contractor or CSP must review the CP testing results and initiate corrective actions. CP testing must include a tabletop exercise and functional testing. A copy of the CP testing results must be provided to the COR within 30 days of test execution along with any documentation and corrective actions to be taken by the contractor.

The results of each CP test must be reviewed and documented. At a minimum, the following items must be included the CP test:

- Name of Test
- Name of System
- Date of Test
- Testing point of contact
- Purpose, Type of Test, and Scope
- Objectives
- Methodology
- Activities and Results (Action, Expected Results, Actual Results)
- Action Item Assessment

18.5 CP-6 Alternate Storage Site

Contractors, including those using CSP's must establish an alternate storage site, including the necessary agreements to permit the storage and retrieval of backup information, backup media, and backup data. All backup information/media/data containing IRS SBU data must be encrypted with FIPS 140-2 or later validated cryptographic modules. The alternate storage site must be physically separated from the primary storage site to reduce susceptibility to the same threats. The alternate storage site must enable recovery of operations and provide information security safeguards equivalent to that of the primary site.

Potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions outlined.

18.6 CP-7 Alternate Processing Site

Contractors, including those using CSP's must establish an alternate processing site, including the necessary agreements to permit the transfer and resumption of information systems operations for essential mission and business functions within specified timeframes consistent with the RTO and RPO.

Contractors, including those using CSP's must ensure that the equipment and supplies required to resume operations at the alternate site are in place, or that required equipment/supplies are made available within specified timeframes, to avoid unacceptable delays in the delivery of contracted services. Alternate processing sites are locations that are sufficiently separated from the primary processing sites to reduce susceptibility to the same threats. The systems, personnel, and physical security controls must be commensurate with the sensitivity of the information being restored, and with the security of the primary processing site.

Potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must be outlined.

Alternate processing site agreements must be developed that contain priority-of-service provisions (e.g., SLA) in accordance with the organization's availability requirements (including the RTO).

The Contractor must develop policies and procedures to safeguard IRS SBU data for work performed at alternate processing sites such as approved telework locations.

Contractors must ensure the following eligibility requirements are met before contractor personnel are approved to telework:

IRS Approval
Contractors must receive approval in writing from the IRS COR or BU before allowing contractor personnel to support the IRS contract from an approved telework location.

Telework Training
Contractor personnel that want to utilize telework to support the IRS contract must complete annual telework training. Telework training can be provided by the contractor.

Signed Telework Agreement
A telework agreement must be utilized to confirm the employee's understanding and acceptance of their responsibilities for protecting IRS SBU data and communicating requirements for a suitable work environment.

The telework agreement at a minimum must include the following information:

- The terms and conditions of the telework arrangement between the voluntarily participating contractor and their organization.

- Telework agreements must be signed/dated by the applicant and include their telework location address, and
- The telework agreement must be signed/dated by the contractor's supervisor/manager. Once signed by management, the applicant is eligible for telework; assuming all other conditions above are met.

Contractors approved to telework must only telework from the approved location and may not telework from any other location without prior management approval. Contractors working at an approved telework location must report all computer security and privacy incidents to management immediately upon discovery. The contractor or the IRS reserve the right to terminate an employee's ability to telework at will.

18.7 CP-8 Telecommunications Services

Contractors, including those using CSP's must ensure that the primary and alternate processing and storage sites have the necessary telecommunications services needed to support the information systems, to resume operations within specified timeframes.

The Contractor, or CSP must develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the Contractor's availability requirements.

The Contractor, or CSP must obtain alternate telecommunications services to reduce the likelihood of a single point of failure with primary telecommunications services.

18.8 CP-9 System Backup

The Contractor must implement backup procedures for all IRS SBU data including user-level information, system-level information, including security and privacy related documentation.

System-level information includes, system-state information, OS and application software, and licenses. User-level information includes any information other than system level information and/or IRS SBU data.

The Contractor must protect the confidentiality, integrity, and availability of backup information at storage locations. The contractor must test backup restoration semi-annually to verify backup reliability and information integrity.

The Contractor must implement FIPS 140-2 or later validated cryptographic modules to prevent unauthorized disclosure and modification of backup information.

If a contractor stores FTI backup data in the cloud, the storage environment must be FedRAMP Authorized at the Moderate or High impact level.

Contractors using a CSP must ensure that they or the CSP will conduct backups for information contained in the information system at the following frequencies:

- User-level: Weekly
- System-level: Weekly
- Information system configuration: Weekly

The Contractor or CSP must maintain:

- At least three backup copies of user-level information (at least one of which is available online) or provide an equivalent alternative.
- At least three backup copies of system-level information (at least one of which is available online) or provide an equivalent alternative.
- At least three backup copies of information system documentation including security information (at least one of which is available online) or provide an equivalent alternative, and
- Backup information must be tested to verify backup reliability and information integrity at least semiannually.

18.9 CP-10 System Recovery and Reconstitution

Contractors, including those using CSP's must ensure that there are procedures in place to provide for the recovery and reconstitution of any IT assets or information system to a known state after a disruption, compromise, or failure within a timeframe consistent with contractor defined RTO and RPO.

Contractors with contracts that support IRS Filing Season systems/processes and/or IRS MEFs, the RPO and RTO defined in the Contractor CP must be the same as the RPO and RTO defined in the IRS MEF CP. The RPO and RTO for IRS Filing Season systems/processes and/or IRS MEFs must be obtained from the COR.

19.0 Identification and Authentication (IA)

Identification and Authentication are the stages of the process that is used to identify an individual (e.g., username) to the information system and authenticate (e.g., password, or token) the individual, prior to allowing access to an IT asset, such as a workstation, laptop, server, etc.

19.1 IA-1 Identification and Authentication Policy and Procedures

Contractors , including those using CSP's must designate an official to manage the development, documentation, and dissemination of the IA policies and procedures for Security and Privacy Controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Policies and procedures must be reviewed/updated annually, or if there is a significant change to IA security controls.

19.2 IA-2 Identification and Authentication (Organizational Users)

Contractors, including those using CSP's must require Identification and Authentication to access IT assets and information systems. Identification must be accomplished by presenting a username to identify the user to the system. Authentication must be accomplished using methods such as passwords, tokens, smart cards, or biometrics.

Supplemental C-SCRM Guidance: Contractors must ensure that identification and requirements are defined and applied for Contractor users accessing an ICT/OT system or supply chain network. A Contractor user may include employees, individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.), and system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The Contractor may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

19.3 IA-3 Device Identification and Authentication

Contractor information systems, including those using CSP's must uniquely identify and authenticate devices before establishing a local, remote or network connection. Organizational devices requiring unique device-to-device IA may be defined by type, device, or a combination of type/device. Information systems typically use one of the following to identify and authenticate devices on local and/or wide area networks:

- Shared known information (e.g., Media Access Control (MAC),
- Transmission Control Protocol/Internet Protocol (TCP/IP) addresses for device identification,
- An organizational authentication solution (e.g., Institute of Electrical and Electronics Engineering (IEEE) 802.1(x), and/or
- Extensible Authentication Protocol (EAP), Radius server with EAP-TLS authentication, Kerberos).

19.4 IA-4 Identifier Management

Contractors, including those using CSP's must manage all identifiers (e.g., usernames) for either systems or IT assets to include the following:

- All default vendor or factory-set administrative accounts and passwords must be changed during installation or immediately after installation.
- Establishing user accounts, only after receiving authorization from an individual assigned and authorized to approve new user accounts, user roles, groups, etc.
- Manage individual identifiers by uniquely identifying everyone with their status. Status identifiers include contractors, subcontractors, etc., and
- Ensuring that user groups establish a naming convention to enable management to understand the creation and management of user accounts, groups, etc.

Supplemental C-SCRM Guidance: Identifiers allow for greater discoverability and traceability. Within the Contractor's supply chain, identifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle – from concept to retirement – but, at a minimum, throughout the system's life within the Contractor.

For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the Contractor's supply chain, such as when they are transferred to the Contractor's ownership or control through shipping and receiving or via download.

Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Contractors must correlate those identifiers with the Contractor-assigned identifiers for traceability and accountability. Contractors must require

their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

19.5 IA-5 Authenticator Management

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time passwords, and ID badges. Device authenticators include certificates and passwords.

The Contractor information system for password-based authentication must implement the following password settings:

- Passwords for Windows-based authentication must contain a minimum of 12 characters for user accounts.
- Passwords for all other systems must contain a minimum 8 characters.
- Passwords for service accounts must contain a minimum of 14 characters.
- All systems enforce password complexity, to contain a combination of letters, numbers, and special characters for all information system accounts.
- For Windows-based systems, enforce a password minimum lifetime restriction of 1 day and maximum of 60 days.
- For all other systems, enforce a password minimum lifetime restriction of 1 day and maximum of 90 days.
- Must prohibit password reuse for 24 generations for Windows-based systems, and 10 generations for all other systems.
- Encrypt passwords in storage and transmission.
- New passwords selected for use must have at least 1 character changed from the previous password.
- Allow the use of a temporary password for system logon, with an immediate change to a permanent password.

CSP issued/managed passwords must be:

- Changed every 60 days
- Complex with a minimum of 14 characters; case sensitive, and at least one each of; upper-case letters, lower-case letters, numbers, and special characters.
- Password enforcement must provide lifetime restrictions of 1 day minimum and 60 days maximum, and
- Passwords must be prohibited from reuse for 24 generations.

For IT devices using a Personal Identification Number (PIN) as an authenticator, the PIN must meet the following requirements:

- Minimum length of 8 digits,
- No repeating digits (e.g., 44444444 or 12121212),
- No sequential digits (e.g., 12345678, 87654321),
- Not be stored with the device, and
- Not be shared.

When Public Key Infrastructure (PKI) is used in the information system, it must:

- Validate certificates by constructing a certification path with status information to an accepted trust anchor, including checking certificate status information.
- Implement a local cache of revocation data to support path discovery and validation, and
- Enforce authorized access to the corresponding private key.

The Contractor must ensure that the information system used to authenticate employees has a backup mechanism able to assume authentication responsibilities in a timely manner if the primary authentication device fails.

The Contractor must require that the registration process to receive Homeland Security Presidential Directive-12 (HSPD-12) PIV card be carried out in person, with a designated registration authority with authorization, by a designated contractor official (e.g., a supervisor). This only applies when contractors are also accessing IRS laptops/systems and/or facilities.

When passwords are lost, the Contractor must ensure there is a process to manage lost passwords to ensure information is not compromised. All vendor passwords or passwords issued with the information systems and applications must be changed, including any default passwords during implementation.

Employees must be trained on the proper handling of individual passwords to prevent unauthorized use or modification.

Users must protect passwords, hardware tokens, and/or smart cards, and ensure they are not stored on, or with a laptop or portable electronic device (PED), unless encrypted or otherwise under the direct and continuous control of the authorized user.

Supplemental C-SCRM Guidance: This control facilitates traceability and non-repudiation throughout the supply chain. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

19.6 IA-6 Authenticator Feedback

Contractors, including those using CSP's must ensure when using password or other authentication mechanisms, the information system or application must generate non-readable characters, such as asterisks to prevent this information from being viewed by unauthorized individuals.

19.7 IA-7 Cryptographic Module Authentication

Contractors, including those using CSP's must ensure when employing cryptographic algorithms for authentication, the encryption algorithms must be FIPS 140-2 or later validated. Current FIPS 140-2 validation lists can be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

When contractors are employing cryptographic algorithms for Kerberos authentication, **AES (128, 192, 256-bit in CBC, CTS, or GCM modes, SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, and HMAC with SHA-2 are the only allowable types.**

19.8 IA-8 Identification and Authentication (Non-Organizational Users)

Contractors, including those using CSP's must ensure when developing or managing public facing websites or portals that require authentication that non-contractor users are uniquely identified and authenticated.

19.9 IA-9 Service Identification and Authentication (C-SCRM Control)

Contractors must ensure web applications querying a database must require unique identification and authentication before establishing communications with devices, users, or other services or applications.

Contractors must ensure that identification and authentication are defined and managed for access to services (e.g., web applications using digital certificates, services or applications that query a database as opposed to labor services) throughout the supply chain. Contractors must ensure that they know what services are being procured and the supplier of the service. Services procured should be listed on a validated list of services for the Contractor or have compensating controls in place.

20.0 Incident Response (IR)

Incident response is the structured approach an organization takes to **identify, manage, and recover from incidents** such as cyberattacks, data breaches, or system outages. The main goal of incident response is to minimize damage, reduce recovery time and costs, and prevent future incidents.

20.1 IR-1 Incident Response Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the IR policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor, or CSP must review/update IR policies and procedures annually, if there is a significant change to IR policies and procedures, or after a security or privacy incident.

Supplemental C-SCRM Guidance: Contractors should integrate C-SCRM into IR policy and procedures, and related C-SCRM Strategy/Implementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybersecurity incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The IR policy should state when and how threats and incidents should be handled, reported, and managed.

Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to inform all involved parties of a supply chain cybersecurity incident. Depending on the severity of the incident, the need for accelerated communications up and down the supply chain may be necessary. Appropriate agreements should be put in place with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure speed of communication, response, corrective actions, and other related activities. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

20.2 IR-2 Incident Response Training

Employees of contractors, including those using CSP's must be trained on IR and reporting procedures at least annually, to understand their responsibilities on reporting security and privacy related incidents and breaches, and how to recognize, report, and respond to a breach (This can be satisfied by completing the IRS provided annual security awareness training, unless additional requirements are defined in the contract).

IR training for contractors assuming an IR role, is required within 30 days of assuming an IR role and responsibility, when required by information system changes, or when acquiring system access, and annually thereafter. Incident response training content must be reviewed and updated every three years and following significant changes.

Incidents that involve SBU/PII are considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses SBU/PII or an authorized user accesses or potentially accesses such information for other than authorized purposes. IR training must emphasize the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. IR training includes tabletop exercises that simulates a breach. IR test results, findings, and plan updates must be shared with the COR within 30 days of completion of the IR training exercise.

Supplemental C-SCRM Guidance: Contractors must ensure that critical suppliers are included in IR training. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

20.3 IR-3 Incident Response Testing

Contractors, including those using CSP's must annually test and/or exercise the IR capability to determine their IR effectiveness and document the results to ensure the security and privacy policies and procedures continue to function, as intended. Contractors and subcontractors must review NIST SP 800-61 Revision 3, Computer Security Incident Handling Guide for guidance on developing and maintaining their IR capabilities. Testing results must be documented, and IR policies and procedures must be updated to close any gaps found in the plan.

IR testing includes reporting phone numbers identified in contractor procedures are accurate; the use of checklists, walk-through, or tabletop exercises; simulations and comprehensive exercises.

IR test results, findings, and plan updates must be shared with the COR within of 30 days of completion of the IR test.

20.4 IR-4 Incident Handling

A security incident as defined by OMB M-17-12 is an occurrence that:

- Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

A data breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses SBU, or
- An authorized user accesses or potentially accesses SBU for other than authorized purpose.

A data breach is not limited to an occurrence where a person other than an authorized user potentially accesses SBU by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment (See **Table 3: Examples of Security and Privacy Incidents**).

Often, an occurrence may first be identified as an incident but later identified as a data breach once it is determined that the incident involves unauthorized access and/or loss of controlled SBU, as is often the case with a lost or stolen laptop or electronic storage device. For the purposes of this section when referring to "incidents" it will include data breaches.

Whenever there is a compromise of IRS information, the Contractor, or CSP must contact the IRS immediately upon discovery of the incident or potential incident. The IRS must work closely with IRS contractors, and CSP's to quickly respond to a suspected incident of unauthorized disclosure or inspection.

Types of incidents include the following:

Table 3: Examples of Security and Privacy Incidents

Incident Type	Description
Denial of Service	An attack that prevents or impairs the authorized use of networks, information systems, or applications by exhausting resources.
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
Unauthorized Access	A person or information system gains logical or physical access without permission to a network, information system, application, data, or other resource.

Inappropriate Usage	A person violates acceptable information system use policies or improper use of SBU data (e.g., IRC § 6713 and 7216).
Multiple Component	A single incident that encompasses two or more incident types.
Theft	Removal of information systems, data/records on information system media or paper files.
Loss/Accident	Accidental misplacement or loss of information systems, data/records on information system media or paper files.
Disclosure of Sensitive Data	Disclosure of sensitive data refers to the unauthorized, inadvertent disclosure of SBU/PII data.

Contractors, including those using CSP's must maintain capabilities to determine what IRS SBU data was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access IRS SBU data, and identify the initial attack vector.

Contractors, including those using CSP's must implement an incident handling capability for security and privacy incidents that includes a procedure describing the process that must be used in the event an incident is detected. Incident handling procedures must document the process used to handle incidents, including preparation, detection and analysis, containment, eradication, and recovery. Incident handling activities must be coordinated with contingency planning activities. Lessons learned from ongoing incident handling activities must be incorporated into IR procedures, training, and testing/exercises, and must implement the resulting changes accordingly.

Contractors, including those using CSP's must routinely track and document security and privacy incidents potentially affecting the confidentiality of SBU or PII data. An incident that involves SBU/PII is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses SBU/PII or an authorized user accesses or potentially accesses such information for other than authorized purposes. Where contractors rely on IT technical support, the contractors must ensure the IT support teams address the need to manage and track incidents.

Automated mechanisms must be employed to support the incident handling process. This includes online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

20.4.1 IR-4 (10) Incident Handling | Supply Chain Coordination (C-SCRM Control)

Contractor must coordinate supply chain incident handling activities with their supply chain providers and the IRS.

20.5 IR-5 Incident Monitoring

Contractor, including those using CSP's, must track and document all security and privacy incidents and data breaches related to IRS SBU. Documenting incidents includes maintaining records about each incident, the status of the incident as well as evaluating incident details, trends, and handling.

Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user & administrator reports.

20.6 IR-6 Incident Reporting

Contractors, including those using CSP's must report a suspected incident or confirmed breach in any medium or form, including paper, oral, and electronic immediately upon discovery.

Automated mechanisms must be employed to assist in the reporting of incidents. Automated reporting mechanisms include email and automated incident response tools.

Security, Privacy and supply chain incidents related to IRS processing, SBU data, or contractor information systems must be reported immediately upon discovery to the:

- CO and COR,
- CSIRC Incident Response Operations Team at (240) 613-3606 or CSIRC@irs.gov
- Within one hour of notification of the incident, the COR must complete the Computer Security Incident Reporting Form available @ https://www.csirc.web.irs.gov/incident/ and
- Within one hour of notification of the incident the COR must notify the CSA team @ it.cyber.csa.request@irs.gov.

Physical incidents must be referred to the Situational Awareness Monitoring Center (SAMC) at (866) 216-4809. In situations where there is a physical security incident involving IRS processing, SBU data, or contractor information systems, both CSIRC and SAMC must be contacted. CSIRC is available 24x7x365.

The COR must report the incident/data breach to the Treasury Inspector General for Tax Administration (TIGTA) hotline at (800) 366-4484 if the incident/data breach:

- Involves FTI,
- Threatens the safety or security of personnel or information systems, and/or
- Involves a **willful**, unauthorized disclosure.

Failure of the Contractor to notify the IRS in the event of an incident within the required timeframe must be considered a breach of contract. The IRS reserves the right to remedies such as termination of the contract or assess liquidated damages as allowed with FAR clause

52.211-11 -- Liquidated Damages -- Supplies, Services, or Research and Development (September 2000).

20.6.1 IR-6 (3) Incident Reporting | Supply Chain Coordination (C-SCRM Control)

Contractors must report supply chain incident information to their supply chain providers and the IRS.

20.7 IR-7 Incident Response Assistance

Contractors, including those using CSP's must identify IR resources (help desk or IR team) who must assist with the handling of potential incidents. The support resources must have adequate training and understanding to help resume business operations, while providing support to contain and manage a potential incident.

Automated mechanisms must be employed to increase the availability of IR related information and support.

Based on the severity and potential impact of an incident, the IRS reserves the right to provide IR assistance. IRS assistance can include inspection, investigation, forensic analysis, and recovery operations. The contractor and subcontractor must provide support and fully cooperate with IRS staff should their services be warranted.

20.7.1 IR-7 (2) Incident Response Assistance | Coordination with External Providers (C-SCRM Control)

Contractors must have automated mechanisms to increase access to IR information and support.

Contractor agreements with prime contractors must specify the conditions under which a government approved or designated third-party would be available or may be required to provide assistance with incident response, as well as the role and responsibility of that third-party.

20.8 IR-8 Incident Response Plan

Contractors, including those using a CSP must develop and annually review an IR plan that provides a high-level approach to handle incidents. The plan must:

- Provide the organization with a roadmap for implementing its IR capability.
- Describe the structure and organization of the IR capability.
- Provide a high-level approach for how the IR capability fits into the overall organization.
- Define reportable incidents.
- Address the sharing of incident information.
- Explicitly designate responsibility for IR to personnel/team.

- Update the IR plan to address system and organizational changes, or problems encountered during plan implementation, execution, or testing.
- Provide metrics for measuring the IR capability within the organization.
- Define the resources and management support needed to effectively maintain and enhance IR capabilities.
- Be reviewed and approved by Contractor Security Representative.
- Protect the IR plan from unauthorized disclosure and modification, and
- Identify data elements involved in the breach.

Supplemental C-SCRM Guidance: Contractors must coordinate, develop, and implement an IR plan that includes information-sharing responsibilities with critical suppliers, and, in a federal context, interagency partners and the FASC. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

20.9 IR-9 Information Spillage Response (C-SCRM Control)

Contractor must include the following in their information response activities:

- Assignment of organizational roles and their responsibility for responding to information spill.
- Identification of specific information involved in the system contamination.
- Alerting IR personnel of the information spill using a method of communication not associated with the spill.
- Isolating the contaminated system or system component.
- Eradicating the information from the contaminated system or component.
- Identifying other systems or system components that may have been subsequently contaminated, and
- Initial IR and subsequent update reporting to both the applicable external service providers and the IRS.
-

21.0 Maintenance (MA)

Maintenance ensures that all IT assets are available and ensures the integrity and reliability of the equipment. Contractors, including those using CSP's must rely on the operation and functionality of equipment if they are to provide continued service to the IRS.

21.1 MA-1 Maintenance Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the MA policy and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update policies and procedures annually, or if there is a significant change describing MA procedures to be used for that contractor site.

Supplemental C-SCRM Guidance: Contractors must ensure that C-SCRM is included in MA policies and procedures and any related SCRM Strategy/Implementation Plan, SCRM Policies, and SCRM Plan(s) for all Contractor information systems and networks. With many MA contracts, information on mission-, Contractor-, and system-specific objectives and requirements is shared between the Contractor and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the MA of systems is outsourced to a system integrator, and as such, appropriate measures must be taken. Even when MA is not outsourced, the supply chain affects upgrades, patches, the frequency of MA, replacement parts, and other aspects of system MA.

MA policies should be defined for both the system and the network. The MA policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms.

The MA policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.

The Contractor should communicate applicable MA policy requirements to relevant prime contractors and require that they implement this control and flow down this requirement to relevant sub-tier contractors.

21.2 MA-2 Controlled Maintenance

Contractors, including those using CSP's establish a formal information systems MA program, that applies to all types of MA to all system components (including but not limited to; applications, servers, workstations, storage arrays, routers, switches, firewalls, scanners, copiers, and printers) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

Changes made to hardware or software during MA must be recorded per configuration management processes for the hardware or software.

The Contractor must maintain a log of all MA to include, at a minimum:

- Date and time of maintenance,
- Name of individuals or group performing the maintenance,
- Name of escort, if necessary,
- Description of the maintenance performed, and
- Information system components/equipment removed or replaced (including identification numbers, serial numbers, and/or barcodes, if applicable).

The Contractor must approve and monitor all maintenance activities, whether the equipment is serviced; on-site, remotely, or removed to another location. Maintenance policy shall identify a maintenance window to obtain maintenance support for information system components in the event of a failure

When off-site maintenance or repairs are required, the CSR must explicitly approve, with an approval letter or form, the removal of system components from the Contractor's facilities. The Contractor must sanitize equipment to remove all information from associated storage prior to removal from the contractor's facilities for off-site maintenance repair, or replacement. Any equipment that cannot be sanitized must be destroyed using media disposal processes contained in this document.

When maintenance or repair actions are completed, on-site or off-site, the Contractor must check all potentially impacted security controls to verify the controls are still functioning properly.

Contractors using a CSP must ensure that the CSP:

- Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications.
- Approves and monitors all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location, and

- Sanitizes equipment to remove all information from associated storage prior to removal from organizational facilities for off-site maintenance or repairs.

21.3 MA-3 Maintenance Tools

Contractors, including those using CSP's must establish, maintain, update and review annually an inventory of approved software, hardware, remote and firmware maintenance tools.

This control addresses security risks related to maintenance tools used for diagnostics and repairs on contractor and CSP information systems. Such tools can serve as vectors for malicious code, whether introduced intentionally or inadvertently.

Before installation or use, all maintenance tools must be scanned for malicious code and inspected for improper or unauthorized modifications. Maintenance tools or equipment with data storage capabilities must be sanitized before removal from contractor facilities.

21.4 MA-4 Non-Local Maintenance

Non-local maintenance and diagnostic activities are those activities conducted by an individual who is communicating through a network using a VPN or zero trust technology to remotely access the contractor's IT assets.

When non-local Maintenance is performed, the following is required:

- A log must be created and maintained to identify all non-local access and maintenance into the contractor's information system.
- All tools used to provide remote maintenance and support must be documented.
- Contractor support personnel must use two-factor authentication or PKI to access the information system remotely. All network communications must be terminated when work is completed.

Contractor and CSP personnel providing IT support must document and periodically review non-local maintenance. The Contractor must document in the SSP the use of non-local maintenance and diagnostic connections.

Supplemental C-SCRM Guidance: Nonlocal MA may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal MA personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar MA role and enforced through contractual agreements with their external service providers. The Contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

21.5 MA-5 Maintenance Personnel

Contractors including those using CSP's must establish a process for authorizing and maintaining a list of maintenance personnel. Non-escorted personnel performing maintenance on the information system must have at least an Interim IRS clearance on file with the COR. The Contractor must designate key personnel with at least an Interim IRS clearance and technical competence to supervise the maintenance activities of personnel who do not have at least an Interim IRS clearance.

21.6 MA-6 Timely Maintenance

The Contractor or CSP must define maintenance support and/or spare parts required for key information technology components to meet the recovery time objective/recovery point objective (RTO/RPO) timelines defined in the Contingency Plan/Disaster Recovery Plan.

22.0 Media Protection (MP)

MP controls ensure that all removable media is adequately secured to allow for the deterrence, detection, reporting, and management in the event of loss, theft, or destruction. An inventory shall be maintained and provided to the IRS, upon request, that identifies all media used to store, maintain, or process IRS SBU data. Media that is used to store, maintain, or process IRS SBU shall not be commingled with non-IRS data. IRS SBU being handled or processed by the Contractor shall be logically and/or physically segregated from other client's data.

22.1 MP-1 Media Protection Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of the MP policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update policies and procedures annually, or if there is a significant change. Events that require an update to MP policy and procedures include assessments, audit findings, and security or privacy incidents.

The MP policies and procedures must describe requirements to restrict access to information system media to authorized individuals when this media contains IRS SBU data. Information system digital media includes, but must not be limited to diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, and DVDs. An inventory must be maintained and provided to the IRS, upon request, that identifies all media used to store, maintain, or process IRS SBU data. Media that is used to store, maintain, or process IRS SBU must not be commingled with non-IRS data. IRS SBU being handled or processed by the contractor must be logically and/or physically segregated from other client's data.

22.1.1 MP-1 Return or sanitization/destruction of hard and softcopy media at the End of Performance, under the Contract.

Within three months prior to the end of the base year of a contract, the Contractor must submit to the COR a plan for the return of all hard and softcopy media (identified below) or for the destruction and/or sanitization of all hard and softcopy media used, purchased specifically by the Contractor for performance under the contract, or provided by the IRS to the Contractor for use in the performance of this contract.

Examples of media that must be returned or will require sanitization and/or destruction include:

- Backups,
- VoIP devices,
- Hard drives,
- Storage Arrays,
- Router, switch, and firewall configurations,
- Network - restored to original settings, and
- Faxes/copiers.

The plan must address the time by which the return of the property will be completed and/or how and when the destruction/sanitization will take place. The contractor may treat different property differently. The COR, in consultation with the CSA Team, will review the plan and inform the Contractor within 30 days of receipt of the plan which option is preferable. The objective of this requirement is to ensure that all IRS SBU data is no longer available to the contractor, its employees, or anyone else not authorized access to the data. The IRS has the option to perform an onsite closeout assessment, remote closeout assessment, or utilize other methods to validate the sanitization and or destruction process. The contractor must send a certification of the sanitization/destruction to the COR before the end of the contract as part of the contract closeout process.

22.2 MP-2 Media Access

Contractors including those using CSP's must ensure that media access is restricted to prevent hard copy media from being lost, stolen, or disclosed. Electronic, optical, and other digital media must be restricted to prevent unauthorized access and disclosure.

Digital media includes but is not limited to; flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), CDs, and DVDs.

Contractors must be made aware of the need to protect and properly secure SBU data against inadvertent disclosure when visitors/maintenance/vendors etc., are in work areas.

An after-hours walk-through must be conducted at least quarterly by the contractor to ensure IRS SBU data is safeguarded after hours.

22.3 MP-3 Media Marking

The Contractor must label all media to identify it contains IRS SBU. Media must be labeled "IRS Data – Sensitive but Unclassified".

Media is exempt from marking when it remains within contractor-controlled areas.

22.4 MP-4 Media Storage

For contractors who house IRS SBU, the Contractor or CSP must physically control and securely store information system media within controlled areas. When this media contains IRS SBU data, the contractor must maintain information in a lockable, metal filing cabinet. When larger volumes of information are being maintained at a contractor site, the Contractor must use automated mechanisms (key card access, biometric access, cipher locks, etc.) to restrict access to media storage areas, and to audit access attempts and access granted.

The Contractor or CSP must employ FIPS 140-2 or later validated cryptographic modules to protect information in storage. Minimum physical security requirements must be met, such as keeping SBU data secured when not in use. Removable media also must be encrypted and labeled SBU data when it contains IRS SBU. For more information see Section **23.0 Physical and Environmental Protections (PE)**.

Information system media must be protected until the media is destroyed, or sanitized using approved equipment, techniques, and procedures.

Records must be established to track all deposits and withdrawals from media storage facilities and libraries.

Business and functional units must establish management controls that ensure all portable mass storage devices are inventoried, administered, and turned in during employee separations or reassignments.

This control applies to media storage areas within organizations, where significant volumes of media are stored, and does not apply to every location where media are stored (e.g., in individual offices).

Supplemental C-SCRM Guidance: Media storage controls should include C-SCRM activities. Contractors must specify and include in agreements (e.g., contracting language) media storage requirements (e.g., encryption) for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The Contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

22.5 MP-5 Media Transport

Contractors including those using CSP's must document all activities associated with the transport of digital media. The contractor must protect and control digital media during transport outside of controlled areas.

Information systems must implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. The cryptographic modules in use, must be FIPS 140-2 or later validated. This applies to both portable storage devices (e.g., USB memory sticks, CDs, DVDs, external/removable

hard disk drives, SSDs) and mobile devices with storage capability (e.g., smartphones, tablets, E-readers).

Chain of Custody records for digital media must be secured, to prevent unauthorized access and manipulation of log information.

Vehicles used to transport media, and paper must be secured to ensure contents cannot be inadvertently removed or lost from the vehicle, (e.g., secured cabs on the back of a truck).

SBU data in hotels must be stored in a locked room safe, or secured in a safe, in the hotel management offices.

22.6 MP-6 Media Sanitization

Contractors including those using CSP's must sanitize information; digital, optical, and paper prior to disposal or release for reuse using techniques and procedures in accordance with NIST SP 800-88, Revision 2, Guidelines for Media Sanitization. Contractors and CSP's must use sanitization tools and products evaluated and approved by either NSA, DHS, or Department of Defense (DoD). For a list of approved NSA evaluated media destruction products refer to https://www.nsa.gov/resources/Media-Destruction-Guidance.

The Contractor or CSP must possess tools and methods to conduct sanitization of digital media that can be used in clear, purge, and destroy operations.

NIST defines three classes of sanitization. These are clear, purge, and destroy based on the definitions below:

- **Clear -** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using methods such as Secure Erase.
- **Purge -** applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques.
- **Destroy -** renders target data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Use of a sanitization class is dependent on the following conditions:

- If the media will not be reused, then it must be destroyed. This applies to CDs, paper, and decommissioned or inoperable disk drives and storage arrays.
- The media must be purged if it will be reused but will be not under the direct physical control of the contractor.
- If the media will be reused and remain under the direct control of the contractor, then the clearing of IRS SBU data is acceptable.

The most common way to clear data is to perform a disk wipe using a software tool that overwrites all sectors of the disk with positive and negative (0 and 1) values. IRS standards require seven overwrites when the data contains FTI, otherwise three passes are acceptable.

Full-disk wipes must be applied to workstations and laptops. Before a contractor information system is disposed of and leaves organizational control, the contractor must clear or purge any sensitive data from the system BIOS. The BIOS must also be reset to the manufacturer's default settings, to ensure the removal of sensitive settings such as passwords or keys.

Partial data clearing can be appropriate for IRS data stored on file servers that also contain other customer information. There are a variety of software tools that can be used to overwrite selected files and folders, thus retaining the data of other customers.

Methods of purging data include overwrite, block erase, and cryptographic erase. Overwrite is the clear method described above but does require a full-disk wipe. Block and cryptographic erase methods are options that are dependent on the device manufacture.

Another purge option is the use of a degausser. A degausser generates a magnetic field that applies a unidirectional alignment to the data recording surface. Degaussing renders many types of devices unusable (and in those cases, degaussing is also a destruction technique).

Degaussing is adequate for sanitizing magnetic media, but it is not adequate for SSDs, flash drives, or optical disks in those cases, you must use other methods like cryptographic erase or physical destruction.

Destruction methods are designed to physically destroy the data through disintegration, pulverization, melting, or incineration. However, bending, cutting, and the use of some emergency procedures (such as using a power drill or hammer) are not acceptable methods of media destruction as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Contractors must destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by IRS approved methods.

Paper shredders can be used to destroy hard copy materials and flexible media such as diskettes once the media are physically removed from their outer containers. In-office shredders must produce crosscut particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller).

Contractors may elect to use an on-site shredding service vendor. Use of these services in lieu of deploying in-office shredders must adhere to the following standards:

- Materials to be shred must be deposited in locked containers with key registration under management control.
- Shredding must be performed on-site under the direct observation of an IRS cleared contractor staff member.
- The shred vendor must hold National Association for Information Destruction (NAID) certification.
- The shred vendor must provide the contractor with a Certificate of Destruction before leaving the facility.

Optical mass storage media includes, but is not limited to CDs, CD - rewritable (CD-RWs), CD - recordables (CD-Rs), and CD - read only memory (CD-ROMs), DVDs and magneto-optical (MO) disks must be destroyed by pulverizing, cross-cut shredding or burning.

A log must be maintained to provide a record of media destroyed.
The log must include:

- The date of destruction
- Content of media
- Identifying serial number
- Type of media (CD, cartridge, etc.)
- Media destruction performed
- Personnel performing the destruction
- Witnesses to the destruction

IRS SBU and paper media that is identified for destruction, must be secured sufficiently so that it is not mistaken for recycling material or general refuse.

The Contractor or CSP must demonstrate that tools and/or contract support is available to provide for sanitizing, degaussing, shredding, or other data destruction methods, sufficient to meet IRS requirements.

Any contractor authorized to perform destruction of IRS SBU data must be approved for interim/final staff-like access or be under escort of an employee who has approved interim/final staff-like access.

Contractors using a CSP must ensure that the CSP annually tests and verifies sanitization equipment and procedures.

Supplemental C-SCRM Guidance: Contractors must specify and include in agreements (e.g., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Media is used throughout the SDLC. Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensuring that information is removed before the media is used, reused, or discarded. For media that contains privacy or IRS SBU, the Contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

22.7 MP-7 Media Use

Contractors, including those using CSP's must restrict the use of writeable removable media and prohibit the use of portable storage devices when such devices have no identifiable owner.

Add-on devices that can record, or transmit sensitive information (e.g., video, sound, Intermediate Frequency (IF), or Radio Frequency (RF)) must be disabled in areas where IRS SBU data is discussed.

Contractors including those using CSP's must prohibit the use of personally owned equipment, software, or media to process, access, or store IRS SBU data, and prohibit connecting privately-owned Portable Electronic Devices (PED) or removable media to an information system used to process, store, or transmit IRS SBU data.

23.0 Physical and Environmental Protection (PE)

PE policy and procedures address the controls in the PE family that are implemented within systems and organizations. Such policies and procedures must be developed with risk management as a focus, considering both security and privacy concerns. This can be a single policy document or multiple policies covering the various controls.

Physical security must be provided for a document, an item, or an area in several ways. These include but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security information systems, fences, identification information systems, and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available. Proper planning and organization must enhance the security while balancing the costs.

The IRS has categorized SBU data as moderate risk. The controls are intended to protect the information and information systems that contain SBU data. It is not the intent of the IRS to mandate requirements to those information systems and/or areas that are not handling and processing SBU data.

23.1 PE-1 Physical and Environmental Protection

The Contractor must designate an official to manage the development, documentation, and dissemination of the physical, environmental, and privacy protection policy and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update policies and procedures annually, or if there is a significant change to PE procedures to be used for that contractor site. Events that require an update to PE policy and procedures include assessment or audit findings, security and privacy incidents or breaches, or changes in applicable laws.

23.2 PE-2 Physical Access Authorization

Designated officials or designees within the Contractor's organization must develop, review, keep current, and approve the access list and authorization credentials, i.e., identification (ID) badges. ID cards issued to employees and the card key inventory must be reconciled at least annually. The access list to the information and areas handling and processing SBU data must

also be updated at least annually. Additionally, the Contractor must have a procedure to issue, manage, and track ID cards for visitors.

Any contractor company with more than 25 total employees must have a photo ID badging system in place. If an inspection is taking place, an employee may be requested to provide verification of identity to an authorized government agent. Media used to create the badges must be safeguarded to prevent unauthorized use. Badge access programming must be performed by an employee with interim or final staff-like access, if completed onsite. If programming is completed offsite at another contractor location, staff-like access is not required if multiple levels of approval are involved. Badges with access to any secure or limited area where SBU data is present must also have a permanent, unique identifier on the badge to visually identify employees with interim or final staff-like access.

The authorization of employees must be reconciled periodically. Any time an employee departs the organization; the access list and ID/access card must be updated so that access is modified or deleted within 18-hours. Employees must be made aware that ID media (identification cards/access cards) must be used for authorized access. All lost/stolen ID/access cards must be reported to management immediately and access revoked within 18 hours.

Contractors using a CSP must ensure that the CSP develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. Review the access lists detailing authorized facility access by individuals at least annually.

Supplemental C-SCRM Guidance: Contractors must ensure that only authorized individuals with a need for physical access have access to information, systems, or data centers (e.g., sensitive or classified). Such authorizations should specify what the individual is permitted or not permitted to do with regard to their physical access (e.g., view, alter/configure, insert something, connect something, remove, etc.). Agreements must address physical access authorization requirements, and the contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Authorization for non-federal employees should follow an approved protocol, which includes documentation of the authorization and specifies any prerequisites or constraints that pertain to such authorization.

23.3 PE-3 Physical Access Control

When designating an area as limited access, it is important to ensure that management controls of the area are in place. This must apply to all areas where access may be made into a secured perimeter. Examples of areas that may require additional protection include stairwell doors and loading dock areas.

The Contractor must control all access points to the facility. This must not apply to areas officially designated as publicly accessible. The contractor must ensure that access is authorized and verified before granting access to areas where IRS SBU is processed or stored.

Prior to authorizing access to facilities and/or areas where IRS SBU is processed, visitors must be authenticated. This does not apply to areas designated as publicly accessible.

The entry control monitor must verify the identity of visitors by comparing the name and signature entered in the register with the name and signature on types of identification such as state issued driver's license, PIV Card, or US Passport. When leaving the area, the entry control monitor or escort must enter the visitor's time of departure. Each register must be closed out at the end of each month and reviewed by the area supervisor/manager.

Whenever visitors enter the area, the contractor must capture the following information: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

Contractors using a CSP must ensure that the CSP enforces physical access authorizations at entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using CSP defined physical access control systems/devices and guards.

See **Appendix D** for additional guidance on physical access controls.

23.4 PE-4 Access Control for Transmission Medium

The Contractor must physically control and monitor access to transmission lines and closets within the contractor facilities using physical safeguards. Security safeguards to control physical access to information system distribution and transmission lines include, for example:

- Locked wiring closets,
- Disconnected or locked spare jacks,
- Protection of cabling by conduit or cable trays, and/or
- Wiretapping sensors.

23.4.1 Transporting IRS Material

Any time SBU data is transported from one location to another, care must be taken to provide safeguards. In the event the material is hand-carried by an individual in connection with a trip or during daily activities, it must be kept with that individual and protected from unauthorized disclosures. For example, when not in use, and when the individual is out of their hotel room, the material is to be out of view, in a locked briefcase or suitcase.

All shipments of SBU data (including electronic, optical, or other removable media and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All SBU data transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. In addition, the address must be contained on both the outer and inner envelope. The inner envelope must be marked SBU with some indication that only the designated official or delegate is authorized to open it.

Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents. All removable media must be encrypted using FIPS 140-2, or later validated encryption modules.

Computers and IT media as well as sensitive information must be secured when in hotel rooms, when hotel room is unattended.

When transporting IRS SBU material, the contractor must ensure that material must always be safeguarded during transport.

Methods to secure material must include, but are not limited to; sealed envelopes, locked/electronically secured media transport containers, etc.

Any information stored in an automobile must be stored in the trunk. If impractical, the information should be covered from view.

Ensure the courier vehicle is locked and secured when in possession of IRS data and/or remittances.

Ensure the vehicles used by the couriers are:

- Maintained in good condition, appearance, and working order.
- Enclosed to ensure the packages and/or containers carried by the vehicle are secure.
- The vehicle must be secured. Vehicle doors must be secured (doors closed and locked) during transportation of the IRS packages or containers. All windows must be up in the vehicle during the transportation of data and remittances, and
- The areas of the vehicles in which the packages and/or containers are placed, must be clear and debris-free. Other items are not to be commingled with the packages and/or containers.

23.5 PE-5 Access Control for Output Devices

The Contractor must control physical access to the information system devices that display IRS SBU or where IRS SBU is handled or processed to prevent unauthorized individuals from observing the display output. Output devices include monitors, printers, scanners, audio devices, fax machines, projection devices, and copiers. Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, covering windows into secure work areas, facing output screens away from walkways, or some combination of the above.

23.6 PE-6 Monitoring Physical Access

The Contractor must monitor physical access to SBU data and the information systems where IRS SBU is stored, to detect and respond to physical security incidents. Physical access logs must be reviewed annually, or upon occurrence/potential indication of an incident. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Physical security Intrusion Detection Systems (IDS) are designed to detect attempted breaches of perimeter areas. IDS can be used in conjunction with other measures to provide forced entry protection for after-hours security. Additionally, alarms for individual and document safety (fire) and other physical hazards (water pipe breaks) are recommended. Alarms must annunciate at an on-site protection console, a central station, or local police station. Physical security IDS include, but are not limited to door and window contacts, magnetic switches and motion sensors designed to set off an alarm at a given location when the sensor is disturbed.

The Contractor must monitor physical intrusion alarms and surveillance equipment. Video Surveillance Systems (VSS) must have monitoring and recording capabilities but are not required to be monitored in real-time. Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email, and text messages, and activating door locking mechanisms.

23.6.1 Monitoring Private Collection Agencies (PCA)

PCA's must have VSS that record all sensitive areas where Taxpayer data is present, including but not limited to mail processing rooms. PCA's must have a secure area for mail processing and securing payments, that is separate from the contractor's other mail processing. Physical security assessments of the mailrooms and mail processing sites must be conducted annually for PCA's.

23.7 PE-8 Visitor Access Records

The Contractor must maintain visitor access records to the facility where the information system resides. Visitor access records are not required for publicly accessible areas. The contractor must limit PII in visitor access records/logs.

The visitor access log must contain the following information:

- Name and organization of the visitor,
- Signature of the visitor,
- Form of identification,
- Date of access,
- Time of entry and departure,
- Purpose of visit, and
- Name and organization of person visited.

Designated officials or designees within the contractor organization must review the visitor access records, at least annually.

Registers or logs for all areas must be maintained for two years.

Contractors using a CSP must ensure that the CSP reviews visitor access logs, at least monthly.

23.8 PE-9 Power Equipment and Cabling

The Contractor must protect power equipment and power cabling for the information system from damage and destruction. Power equipment and cabling include internal cabling, uninterrupted power sources in offices or data centers, generators, power sources for self-contained components such as satellites, vehicles, or other deployable systems.

23.9 PE-10 Emergency Shutoff

The capability to shut off power to the information system or individual system components in emergency situations must be provided. Access to the shutoff switches or devices must be unobstructed and located in such a manner so personnel have safe and easy access to them. The shutoff switches or devices are to be protected from unauthorized or inadvertent activation.

23.10 PE-11 Emergency Power

The Contractor must provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a loss of primary power. Emergency power can be in the form of an internal Uninterruptible Power Supply (UPS) and/or a backup generator.

23.11 PE-12 Emergency Lighting

The Contractor must employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage that covers emergency exits and evacuation routes within the facility.

23.12 PE-13 Fire Protection

The Contractor must maintain fire suppression, detection, and notification (alarms) devices for the information and/or information systems.

Class A and Class C fire extinguishers must be prominently located within any office complex containing IT assets so that an extinguisher is available within 50 feet of travel. Devices must be supported by an independent power source and appropriate for the size of the facility being protected/safeguarded.

- The Contractor must employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

- When the facility is used to store large volumes of SBU data in warehouses and/or storage facilities, the contractor must ensure thatsprinkler systems and/or water suppression equipment must be in place to minimize damage to critical historical files.

23.13 PE-14 Environmental Controls

The Contractor must maintain and monitor temperature levels within the facility where the information system resides. The monitoring of the temperature levels must generate alerts or notifications when changes in temperature are potentially harmful to personnel or equipment. The alarm or notification may be an audible alarm, visual message, text, or email in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely IR.

23.14 PE-15 Water Damage Protection

The Contractor must protect the information systems from damage resulting from water leakage by ensuring that master shutoff or isolation valves are accessible, working properly and known to key personnel.

23.15 PE-16 Delivery and Removal

For all IT information systems that house SBU data, the contractor must authorize and control information system-related items entering and exiting the facility and maintain appropriate records of those items.

The authorization process must define individuals who are authorized to remove IT related equipment and/or other records.

If mailrooms are used, controls must be put in place to ensure mail is also controlled, once received. (See **Appendix D** for additional guidance of physical access controls of SBU and PII material, and VSS requirements specific to PCA mail processing rooms).

23.16 PE-17 Alternate Work Site

The processing or storage of FTI is restricted to locations as prescribed in **Appendix D**. FTI cannot be processed or stored at employee's home or elsewhere except as otherwise approved by the IRS.

Digital assistants (sometimes called smart devices) and other devices such as smart phones that can record or transmit sensitive audio or visual information must not be allowed to compromise privacy in the work or telework environment. These devices typically contain sensors, microphones, cameras, data storage components, speech recognition, GPS options, and other multimedia capabilities. These features could put the privacy of contractors, employees and/or Taxpayers at risk due to the personal information that might be unwittingly disclosed. When working on any form of SBU data, (including PII and tax information), these rules must be followed:

- Treat the device as if it were another person in the room because many such devices and applications can record and/or transmit data when activated. To protect privacy, contractors must mute or disable the listening/detecting features of the device so that SBU data is not sent to the device or anything to which it is connected.
- If the device or application can take photos or record video or sound, then the contractor must not do sensitive work within visual or audio range.

These devices/applications include (but are not limited to the examples provided):

- Digital assistants (such as Dot or Echo hardware using Alexa software, HomePod using Siri, etc.),
- Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets, etc.),
- Internet-connected toys (Cloud Pet, Smart Toy, Hello Barbie, etc.) that might record and transmit,
- Security systems and webcams in the telework environment,
- Smart TVs or auxiliary equipment (if includes voice activation),
- Operating systems/applications (such as Windows 11, Cortana, etc.) that allow voice commands,
- Home surveillance, security, and video/audio: Webcams on personal devices in the home, security cameras/microphones, and/or
- Smart phones with video/audio capabilities.

Contractor personnel approved telework location must have the following features/capabilities:

- A telephone,
- A workspace suitable to perform work,
- All SBU data in the possession of the employee, must be kept in a locking file cabinet or drawer, laptops must be locked in place or in a locked room,
- Secure remote network access via a VPN, and
- A work environment that is free from interruptions and provides reasonable security and protections.

23.17 PE-23 Facility Location (C-SCRM Control)

Contractors must consider the physical and environmental hazards associated with their current location in their organizational risk management strategy.

Contractors must incorporate the facility location (e.g., data centers) when assessing risks associated with suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations.

Contractors must also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors.

For critical vendors or products, contractors must specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts.

24.0 Planning (PL)

The Contractor is responsible for planning for the security and privacy of IRS SBU and IT assets throughout the life of the contract. Contractors, including those using CSP's must ensure all security and privacy controls have been implemented and provide assurance to the IRS that the controls are in place and functioning.

24.1 PL-1 Planning Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of security and privacy PL policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update policies and procedures annually or if there is a significant change.

24.2 PL-2 System Security and Privacy Plans

Contractors including those using CSP's must develop and maintain a security plan to identify key information about the information system and about security and privacy controls that must be used to ensure that IRS SBU data is adequately safeguarded.

The SSP must:

- Describe the operational context of the information system in terms of missions and business processes.
- Explicitly define the authorization boundary for the system.
- Identify the information types processed, stored, and transmitted by the system.
- Identify contractor personnel that fulfill system roles and responsibilities.
- Describe specific threats to that are concern to the contractor for this information system.
- Identify risk determinations for security and privacy architecture and decisions.
- Provide the results of a privacy risk assessment for systems processing PII.
- Describe the operational environment for the information system and relationships with or connections to other information systems.
- Provide an overview of the security and privacy requirements for the system.

- Describe the security and privacy controls in place or planned for meeting those requirements, and
- Be reviewed and approved prior to plan implementation.

The Contractor or CSP must:

- Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel.
- Review the SSP at a minimum annually or if a significant change occurs.
- Update the SSP to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments, and
- Protect the SSP from unauthorized disclosure and modification.

The SSP must include or reference a plan for media sanitization and disposition that addresses all system media and backups.

The Contractor must plan and coordinate security-related activities affecting the information system with appropriate contractor groups/organizations before conducting such activities to reduce the impact on other contractor entities.

Supplemental C-SCRM Guidance: The SSP must integrate C-SCRM. The Contractor may choose to develop a stand-alone C-SCRM plan for an individual system or integrate SCRM controls into their SSP. The SSP and/or system-level C-SCRM plan provide inputs into and take guidance from the C-SCRM Strategy and Implementation Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2.

The Contractor must coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For example, building and operating a system requires a significant coordination and collaboration between the contractor and system integrator personnel. Such coordination and collaboration should be addressed in the SSP or stand-alone C-SCRM plan. These plans must also consider that suppliers or external service providers may not be able to customize to the acquirer's requirements.

It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for contractor systems that are processing IRS SBU and flow down this requirement to relevant sub-level contractors.

24.3 PL-4 Rules of Behavior

The Contractor must develop a set of expected rules of behavior when processing or handling IRS SBU data. For all contractor employees who have access to IRS SBU data, the Contractor employee must provide a signed acknowledgement indicating their understanding and expected behavior for information and system usage, security, and privacy. The rules of behavior only need to be re-signed by the users if/when they are updated. User acknowledgement of the rules of behavior must be made annually by contractor personnel

who have access to contractor managed IT assets. The rules of behavior must be reviewed annually and updated as necessary by the contractor.

The Contractor must include in the rules of behavior, restrictions on the posting of IRS SBU data on public websites, as well as the use of IRS identifiers (e.g., email addresses) and IRS authenticators (e.g., passwords) on external sites/applications.

The Contractor must establish usage restrictions and implementation guidance for using internet-supported technologies (e.g., websites, instant messaging, social media, social networking sites,) based on the potential for these technologies to cause damage, or disruption to the information system.

Any failure to comply with the rules of behavior must be considered a security and or privacy incident. If the incident is deemed willful, it must be escalated to a security and/or privacy violation and is subject to disciplinary action.

24.4 PL-8 Security and Privacy Architectures

Contractors including those using a CSP must develop and maintain an information security and privacy architecture document that:

- Describes the overall security and privacy architecture of the organization.
- Describes the overall security and privacy architecture supporting the IRS contract.
- Describes or shows the IRS SBU data flow (data flow diagram).
- Describes the requirements and approach to be taken for processing PII, to minimize privacy risk to individuals.
- Describes the overall philosophy, requirements, and approach to be taken regarding protecting the confidentiality, integrity, and availability of contractor information.
- Describes how the information security architecture is integrated into and supports the enterprise architecture, and
- Describes any information security assumptions about, and dependencies on, external services.

The security and privacy architecture document must be reviewed and updated annually to reflect updates in the enterprise architecture.

Planned information security architecture changes must be reflected in the security and privacy plans, the security Concept of Operations (CONOPS), criticality analysis, organizational procedures, and organizational requirements that result in procurements/acquisitions.

25.0 Program Management (PM)

Contractors must develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of IRS SBU processed, stored, and transmitted by contractor information systems; to protect individuals' privacy. The PM controls have been designed to facilitate organizational compliance with IRS security and privacy requirements.

Organizations document PM controls in the information security and privacy program plans. The organization-wide privacy program plan (see PM-18) supplements an organization's SSP. Together, the system security and privacy plans for the individual information systems and the information security and privacy program plans cover the totality of security and privacy controls employed by the organization.

25.1 PM-5 Inventory of Personally Identifiable Information

Contractors must establish, maintain, and update annually an inventory of all systems, applications, and projects that process personally identifiable information. The inventory must support the mapping of data actions, providing individuals with privacy notices, maintaining accurate PII and limiting the processing of PII when such information is not needed for operational purposes. Contractors may use this inventory to ensure that systems only process the PII for authorized purposes and that this processing is still relevant and necessary for the purpose specified within the PCLIA.

Supplemental C-SCRM Guidance: Having a current system inventory is foundational for C-SCRM. Not having a system inventory may lead to the Contractor's inability to identify system and supplier criticality, which would result in an inability to conduct C-SCRM activities. To ensure that all applicable suppliers are identified and categorized for criticality, contractors must include relevant supplier information in the system inventory and maintain its currency and accuracy. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

25.2 PM-18 Privacy Program Plan

Contractors must develop and disseminate an organizational-wide privacy program plan that provides an overview of their privacy program, that:

- Upholds the privacy requirements outlined in the IRS contract and IRS Publication 4812.
- Provides an overview and description of the privacy program.
- Provides for ongoing awareness and monitoring of the privacy controls.
- Includes the role of the contractor's privacy official and their responsibilities.
- Describes management commitment and compliance to the objectives of the privacy program, and
- Is reviewed/updated annually and signed by the privacy official with responsibility and accountability for privacy risks.

Supplemental C-SCRM Guidance: The privacy program plan must include C-SCRM. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

25.3 PM-19 Privacy Program Leadership Role

Contractors must appoint a privacy officer that has at least an interim IRS background investigation on file with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks associated with the IRS contract.

25.4 PM-20 Dissemination of Privacy Program Information

Contractors must post a link to the relevant privacy policy on any known major entry points to the website, application, or digital service. Contractors must provide a link to the privacy policy on any webpage, mobile application or digital service that collects personally identifiable information.

Contractors must develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

- Are written in plain language and organized in a way that is easy to understand and navigate.
- Provide information needed by the public to make an informed decision about whether and how to interact with the organization, and
- Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

25.5 PM-25 Minimization of PII Used in Testing, Training, and Research

The Contractor must develop and implement policies and procedures that forbid the use of IRS PII for internal testing, training, and research without the explicit permission from the IRS.

The Contractor must fictionalize taxpayer names and addresses in training and testing materials to ensure that Taxpayer information is not accidentally released, and disclosure laws are not violated.

Examples of acceptable PII fictionalization:

- For names use categories of objects, such as animals or minerals: Mr. Bass, Ms. Silver, etc.
- For Social Security Numbers, begin fictitious numbers with “0” or “X”: 000-123-4567, etc.

25.6 PM-26 Complaint Management

The Contractor must notify the COR within 5 business days of any privacy-related complaints from the public and cooperate with any subsequent investigation.

Contractors must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

- Mechanisms that are easy to use and readily accessible by the public.
- All information necessary for successfully filing complaints.
- Tracking mechanisms to ensure all complaints received are reviewed and addressed within a contractor defined time-period.
- Acknowledgement of receipt of complaints, concerns, or questions from individuals within contractor defined time-period, and
- Response to complaints, concerns, or questions from individuals within a contractor defined time-period.

Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms.

The information necessary for successfully filing complaints includes:

- Contact information for the senior agency official for privacy or other official designated to receive complaints.
- Privacy complaints may also include PII which is handled in accordance with relevant policies and processes.

26.0 Personnel Security (PS)

All contractor personnel performing or proposed to perform under the contract must be identified to the IRS at time of award to initiate appropriate background investigations. Any contractor personnel who are not favorably adjudicated or otherwise pose a security risk must be immediately removed from the IRS contract, and suitable replacement personnel agreeable to the IRS must be provided.

26.1 PS-1 Personnel Security Policy and Procedures

The Contractor must designate an official to manage the development, documentation, and dissemination of the PS policies and procedures and review/update them annually, or if there is a significant change.

The policy must define the need for all contractor personnel to obtain interim or final staff-like access before beginning work on the IRS contract.

Supplemental C-SCRM Guidance: At each level, the PS policy and procedures and the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan(s) need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. These roles also need to state acquirer personnel responsibilities about relationships with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Policies and procedures need to consider the full SDLC of systems and the roles and responsibilities needed to address the various supply chain infrastructure activities. The contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

26.2 PS-2 Position Risk Designation

At the start of any contract, the Vendor POC will assist the COR with identifying position duties, level of access required, and preliminary assessments of the position risk designation for each type of position performing work on the contract. The POC/COR will complete the Position Designation Survey and will update the information into the Contract Management Module (CMM) System. The Associate Director of Personnel Security has the ultimate authority for position risk designation and may adjust the risk level, if deemed appropriate. The COR must coordinate within the IRS to ensure that all positions have been appropriately risk categorized, as required.

IRS contracts where contractors process, store, or manipulate IRS SBU data must be categorized as moderate risk or high if the IRS deems appropriate, and require that all contractors with access to IRS SBU data attain IRS approved staff-like access through PS. IRS approved staff-like access (interim or final) is also required for any personnel who configure computers, IT assets, or computer systems for the contractor, manage servers in an administrative capacity, have access to maintain and manage routers, or in any other way can

access IRS SBU data and facilities housing IRS SBU data. This would include contractors who design, operate, repair, and/or maintain information systems, and/or require access to IRS SBU data.

Contractors using a CSP must assign a risk designation to all positions; establish screening criteria for individuals filling those positions and ensure that the CSP reviews and updates position risk designations at a minimum every three years.

26.3 PS-3 Personnel Screening

Personnel screening must take place for all contractor personnel who work on IRS contracts. This includes employees who; perform data entry, develop, or write software, perform assessments for tax purposes, perform security or telecommunications design/administration to the information system, create and maintain information system policies or procedures, architectural diagrams, and system security documentation, or have staff-like access to IRS SBU data or information systems. This includes subcontractors who support the prime contractor .

The Contractor must identify to the COR, all contractor staff that will:

- Work on the contract,
- Have access to or handle IRS SBU data, or
- Have access to, operate, or work with information systems containing IRS SBU data.

In addition, the Contractor will identify which contractor staff has or has not completed the current annual requirements for SAT.

Supplemental C-SCRM Guidance: To mitigate insider threat risk, personnel screening policies and procedures must be extended to any contractor personnel with authorized access to information systems, system components, or information system services. Continuous monitoring activities should be commensurate with the contractor's level of access to IRS SBU, PII or FTI information and should be consistent with broader Contractor policies. Screening requirements must be incorporated into agreements and flow down to sub-tier contractors.

26.3.1 PS-3 Eligibility

Contractor personnel, who are assigned to IRS contracted work, must meet the following standards -

Contractor personnel must meet minimum citizenship requirements:

- Contractor personnel designated as high risk must be a US citizen.
- Contractor personnel designated as moderate risk must be a US citizen or Lawful Permanent Resident (LPR), with a minimum of three years of US residency as an LPR, and no break of US residency of a year or more.

- Contractor personnel designated as low risk must be a US Citizen or LPR.
- Contractor personnel must be federally fully tax compliant and must remain compliant for the time they are on the contract, and
- All males born after 1959 must be registered with the Selective Service. If not registered or exempt, the contractor must have a Status Information Letter from the Selective Service.

26.3.2 PS-3 Suitability

Suitability is defined as a person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the IRS. All contractor personnel are subject to a background investigation to determine their suitability and fitness to work on an IRS contract, which includes access to: Treasury/Bureau information; IT and systems; facilities; and/or assets. Investigations include a Federal Bureau of Investigations (FBI) fingerprint screening and a variety of written, electronic, telephonic, or personal contact checks to determine an individual's suitability and eligibility to work on federal contracts. The investigation must be favorably adjudicated.

For contractor-managed resources housing IRS information outside the IRS network, staff-like access must only be granted to contractor personnel who have been deemed by IRS to be eligible and suitable. The Contractor is responsible for ensuring that only authorized personnel have access to these resources, that these authorized personnel understand how to protect the resources, that access requirements are reviewed, and adjustments are made as authorized personnel change job duties, and that access is removed for any authorized personnel who are no longer assigned to IRS contract work. The Contractor must advise the IRS of any changes made to authorized personnel access privileges.

The Contractor must screen individuals prior to authorizing access to the information system. Only individuals who have been granted interim or final staff-like access must be allowed access to IRS SBU data.

26.4 PS-4 Personnel Termination

When contractor personnel leave the IRS contract, the Contractor POC, within one business day, is responsible for notifying the COR. The COR is then responsible for notifying IRS PS. The COR completes the Form 14604 and will separate the Contractor within the CMM, the Contingent Worker Module, and by completing the Separation Clearance Records (SCC) as applicable. Once completed, the COR will forward the Form 14604 to PS. If the COR is unable to access CMM, the COR will forward the Form 14604 to PS for complete separation action. PS will cancel any pending investigations or adjudications and update the security file. Even if the background investigation is already completed, notification is required so that the separation information can be appropriately recorded in the security file. The COR must verify that the subject's access to contractor information system is terminated and ensure all government furnished equipment has been returned to the IRS. Upon termination of any user who has elevated privileges, access must be immediately revoked. For non-privileged users the contractor must disable system access within 1 hour of termination. The COR must gather

any authenticators/credentials associated with the individual, and ensure they are terminated/revoked.

Contractors using a CSP must ensure that they disable system access that is no longer required within 24 hours.

26.5 PS-5 Personnel Transfer

When a contractor transfers on or off the contract, the contractor POC, within one business day, is responsible for notifying the COR. The COR is then responsible for notifying IRS PS. The Contractor POC must review logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the contractor organization, and, when warranted, retrieve all security-related contractor information IT asset-related property; and retain access to contractor information and information systems formerly controlled by a transferred individual. The Contractor POC must work with the COR to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. This must include a new assessment of the risk associated with the new position. If the duties of the new position are designated at a higher risk level (moving from a low-risk position to a moderate risk, or a moderate risk to a high risk), the subject must be re-investigated at the new risk level.

Contractors using a CSP must ensure that they disable system access that is no longer required within 24 hours.

26.6 PS-6 Access Agreements

The Contractor must ensure that individuals requiring access to IRS SBU data and information systems containing IRS SBU data sign a Non-Disclosure Agreement (NDA) and information system access agreements prior to being granted access to IRS SBU data. The COR must at the time of the CSA, must provide a sample of NDAs for the contract to ensure they have been reviewed within the past year and are valid and accurate.

The Contractor must:

- Develop and document access agreements for contractor information systems, and
- Review and update the access agreements annually.

Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with contractor information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements.

Supplemental C-SCRM Guidance: The Contractor must define and document access agreements for all contractors or other external personnel who may need to access the contractor's data, systems, or network, whether physically or logically.

Access agreements must state the appropriate level and method of access to the information system and supply chain network. Terms of access should be consistent with the Contractor's information security policy and may need to specify additional restrictions, such as allowing access during specific timeframes, from specific locations, or only by personnel who have satisfied additional vetting requirements.

The Contractor must deploy audit mechanisms to review, monitor, update, and track access by these parties in accordance with the access agreement. As personnel vary over time, the Contractor must implement a timely and rigorous PS update process for the access agreements. When information systems and network products and services are provided by an entity within the Contractor, there may be an existing access agreement in place. When such an agreement does not exist, it should be established. The Contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

26.7 PS-7 External Personnel Security

The Contractor must establish PS requirements, including security roles and responsibilities for subcontractors. Subcontractors PS requirements must be documented and monitored for compliance. The Contractor must monitor subcontractor compliance and require providers to notify the prime contractor, who will notify IRS COR of any personnel transfers or terminations of subcontractor personnel who possess contract credentials and/or badges, or who have information system privileges. Subcontractors providing IT support must meet the PS requirements of the prime contractor, as they have staff-like access to IRS SBU data.

26.8 PS-8 Personnel Sanctions

A formal sanctions process for contractor personnel failing to comply with information security and privacy policies and procedures must exist and be followed. The Contractor must notify the COR within 1 business day when a formal employee sanctions process is initiated, identifying the individual sanctioned, and the reason for the sanction.

27.0 PII Processing and Transparency (PT)

PT policy and procedures address the controls in the PT family that are implemented within IT systems. PT policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of PT policy and procedures. Procedures can be documented in system security and privacy plans or in one or more separate documents.

27.1 PT-1 PII Processing and Transparency Policy and Procedures

The Contractor must develop, document, and disseminate PT policy and procedures to all contractor personnel with access to PII. Contractors must review/update policies and procedures annually, or if there is a significant change to ensure adequate PT controls are developed and implemented.

Supplemental C-SCRM Guidance: Contractors must ensure that supply chain concerns are included in PT policies and procedures, as well as the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies.

The procedures can be established for the security and privacy program in general and individual information systems. These policy and procedures should address the purpose, scope, roles, responsibilities, management commitment, coordination among contractor entities, and privacy compliance to support systems/components within information systems or the supply chain.

Policies and procedures need to be in place to ensure that contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, how long it can be kept, and what happens to it at the end of a contract. When working with a new supplier, ensure that the agreement includes the most recent set of applicable security requirements. Contractors need to abide by relevant laws and policies regarding information (PII and other sensitive information). The contractor must require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

27.2 PT-2 Authority to Process PII

Contractors must restrict the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of IRS PII to only that which is authorized within the PCLIA or contract.

27.3 PT-3 PII Processing Purposes

Contractor must ensure that PII is processed only for identified purposes, including monitoring, and auditing organizational processing of PII.

Contractor must:

- Describe the purposes in the public privacy notices and policies of the organization, and
- Restrict the access of PII to only that which is compatible with the identified purposes.

Identifying and documenting the purpose for processing provides contractors with a basis for understanding why PII may be processed. The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal.

27.4 PT-5 Privacy Notice

The Contractor must ensure that all forms, web pages, and all other means of collecting personal information on behalf of the IRS include a Privacy Notice and Privacy Act Statement that provides formal notice to individuals from whom the information is collected.

Privacy notices help inform individuals about how their PII is being processed by the system or organization. Privacy notices inform individuals about how, under what authority, and for what purpose their PII is processed. To help individuals understand how their information is being processed, contractors must create materials in plain language.

27.5 PT-7 PII - Social Security Numbers (SSN)

Federal law and policy establish specific requirements for contractors who process or store SSNs. Contractors must take steps to eliminate unnecessary uses of SSNs and contact privacy about the applicability of Form 14132.

When a contractor processes SSNs, they must:

- Eliminate the unnecessary use of SSNs,
- Not deny any right, benefit, or privilege. This does not apply when the SSN is required by federal statute, as it is in IRC 6109 and 5 USC,
- Inform taxpayers and personnel that their SSN is mandatory under tax or employment law, and how we will use it, and
- Not maintain records of how individuals exercise their Constitutional First Amendment rights except as specifically authorized.

28.0 Risk Assessment (RA)

RA controls ensure that risk can be assessed within the contractor's information system or CSP environment, and that appropriate mitigation controls can be implemented.

28.1 RA-1 Risk Assessment Policy and Procedures

Contractors including those using CSP's must designate an official to manage the development, documentation, and dissemination of the RA policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor or CSP must review/update the policies and procedures annually, or if there is a significant change to facilitate implementing RA controls. Such RA controls include risk assessments and updates to risk assessments.

28.2 RA-2 Security Categorization

Contracts containing SBU data for tax administration purposes must be assigned a security categorization of Moderate, unless the IRS determines they should be categorized as High. This security categorization has been established by the IRS in accordance with federal laws, executive orders, directives, policies, regulations, standards, and specifically FIPS 199.

28.3 RA-3 Risk Assessment

Risk Assessments are the process to identify potential threats to or vulnerabilities in the information system, and analyze what the impact to the organization is, if the threat or vulnerability occurred. The following are examples of items that must be evaluated during an RA, where potential threats or vulnerabilities may occur:

- Assignment of roles and responsibilities
- User training
- Assignment of elevated privileges
- Accountability of assets
- Supply chain
- Remote access
- Continuity of operations

RAs use threat sources and events as input for assessment. The following are examples of threat sources and events for assessing:

- Accounts with elevated privileges
- Incorrect privilege settings
- Mishandling of information by privileged users
- Natural disasters
- Environmental failures

A RA must be conducted by the contractor or CSP to assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of IRS SBU data and information systems that support the IRS contract. In addition, an RA must consider supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code.

The Contractor must integrate RA results and risk management decisions from the organization and mission or business process perspectives with system-level RAs.

The Contractor or CSP must document, review, and update the RA results annually or whenever there is a significant change to the information system.

Examples of significant changes to an information system that trigger a RA include:

- Installation of a new, or upgraded OS, middleware component, or application.
- Modifications to system ports, protocols, or services.
- Installation of a new or upgraded hardware platform or firmware component.
- Modifications to cryptographic modules or services, and/or
- Migration from contractor owned and/or operated infrastructure to a CSP.

28.4 RA-5 Vulnerability Monitoring and Scanning

Vulnerability monitoring and scanning help organizations detect weaknesses in their IT environments before they can be exploited by malicious actors vulnerability scanning and monitoring software must be configured to inspect systems for missing updates, patches, and common configuration problems. Vulnerability scanning software must be configured to update the list of information system vulnerabilities scanned and perform authenticated scanning. All workstations, servers, network devices, mobile devices, switches, and routing devices must undergo monthly vulnerability scanning.

The Contractor or CSP must employ vulnerability monitoring solutions that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for; enumerating platforms, software flaws, and improper configurations formatting, checklists and test procedures; and measuring vulnerability impact. The vulnerability monitoring tools must express vulnerabilities in the Common Vulnerabilities and

Exposures (CVE) naming convention and employ the Open Vulnerability and Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

When providing programming services or hosting applications and/or services, contractors must utilize enhanced vulnerability scanning software. Enhanced vulnerability scanning software must inspect source code for common security flaws and performing dynamic build testing that inspects the application for security flaws in run-time. Prior to deployment or delivery, static source code analysis and dynamic build testing must be performed. Enhanced vulnerability scanning must be performed whenever code changes are made, and dynamic build testing must be performed monthly.

At the direction of the CSA Team, the Contractor or CSP must send monthly vulnerability scan results in comma-separated value (CSV) format, for all critical, high, and moderate vulnerabilities detected in the information system to the IRS COR who will share the results with the CSA Team.

The CSV file must be the original information exported by the vulnerability scanning tool and include the following information: the scan summary results showing the number of critical, high, and moderate vulnerabilities and the listing of critical, high, and medium vulnerabilities that include the CVE reference.

The output and results of monthly vulnerability scanning, static source code analysis, and dynamic build testing must be retained for the duration of the contract to support security assessment trend analysis and provided to the COR or CSA Team upon request.

Vulnerabilities must be prioritized for remediation based on risk (highest to lowest). Newly discovered vulnerabilities must be added to the list of vulnerabilities to be scanned prior to a new scan, to ensure that the contractor will take steps to mitigate those vulnerabilities in a timely manner.

Vulnerabilities identified on the scan reports must be remediated within the following time frames:

- Critical - vulnerabilities must be mitigated within 30 days from the date of discovery,
- High - vulnerabilities must be mitigated within 60 days from the date of discovery,
- Medium - vulnerabilities must be mitigated within 120 days from the date of discovery, and
- Low - vulnerabilities must be mitigated within 180 days from the date of discovery.

As part of the vulnerability remediation process, the Contractor must identify if a vulnerability is a false positive and develop a remediation plan to correct the vulnerability.

Contractors using a CSP must ensure that they or the CSP scan information systems and hosted applications (i.e., OS/infrastructure, web applications, and databases) for

vulnerabilities at least monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported.

Contractors using a CSP must ensure that they or the CSP remediate vulnerabilities using the following timeframes:

- Critical - vulnerabilities must be mitigated within 15 days from date of discovery.
- High- vulnerabilities must be mitigated within 30 days from date of discovery, and
- Medium vulnerabilities must be mitigated within 90 days from date of discovery.

Supplemental C-SCRM Guidance: Vulnerability monitoring must cover suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in the contractor's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to suppliers, as well as the information systems, system components, and raw inputs that they provide through the cybersecurity supply chain. Vulnerability monitoring activities should take place at all three levels of the Contractor. Scoping vulnerability monitoring activities requires contractors to consider suppliers as well as their sub-suppliers. Contractors, where applicable and appropriate, may consider providing customers with a Vulnerability Disclosure Report (VDR) to demonstrate proper and complete vulnerability assessments for components listed in SBOMs. The VDR should include the analysis and findings describing the impact (or lack of impact) that the reported vulnerability has on a component or product. The VDR should also contain information on plans to address the CVE. Contractors must consider publishing the VDR within a secure portal available to customers and signing the VDR with a trusted, verifiable, private key that includes a timestamp indicating the date and time of the VDR signature and associated VDR. Contractors must also consider establishing a separate notification channel for customers in cases where vulnerabilities arise that are not disclosed in the VDR. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

28.5 RA-8 Risk Assessment – Privacy Impact Assessments

The Contractor must work with the IRS COR to conduct privacy impact assessments for systems or programs before:

Initiating a new collection of IRS SBU data that includes IRS SBU data permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

The IRS COR and IRS Project Manager must coordinate with the Contractor to complete an IRS PTA. The IRS PTA is used to determine if the Contractor processes IRS SBU (including PII and tax information) and requires a PCLIA. Additionally, the IRS COR and IRS Project Manager must coordinate with the contractor to complete or update a PCLIA within PIAMS. The IRS COR in collaboration with the contractor must update the PCLIA every three years, or when a change creates new privacy risks.

28.6 RA-9 Critically Analysis (C-SCRM Control)

Contractors must ensure critical system components and functions are identified by performing a criticality analysis for systems, system components, or system services at decision points in the SDLC, such as when an architecture or design is being developed, modified, or upgraded.

Contractors must complete a criticality analysis as a prerequisite input to assessments of cybersecurity supply chain risk management activities. First, contractors must complete a criticality analysis as part of the frame step of the C-SCRM Risk Management Process. Then, findings generated in the assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other assess step activities in that they inform and enhance one another.

29.0 System and Services Acquisition (SA)

SA controls ensure that security and privacy are incorporated into the IT environment whenever IT assets are being evaluated and/or procured for use.

29.1 SA-1 System and Services Acquisition Policy and Procedures

Contractors including those using CSP's must designate an official to manage the development, documentation, and dissemination of the SA policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

Contractors must review/update policies and procedures annually, if there is a significant change, or following certain events including assessment or audit findings and security or privacy incidents; to ensure adequate information SA policies are developed and implemented.

Information assurance must be considered a requirement for all systems used to enter, process, store, display, or transmit IRS SBU data. Information assurance provides for the availability of systems, ensures the integrity and confidentiality of information, and the authentication/non-repudiation of parties in electronic transactions.

29.2 SA-2 Allocation of Resources

The Contractor must ensure that security and privacy capabilities are procured to be used in conjunction with IT capabilities for IT assets, such as laptops, workstations, or servers.

If the Contractor is managing a network or information system, they must ensure the need for security tools is assessed as requirements are developed for procurement for IT components. The Contractor must determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the IT information system and/or application programs.

The Contractor must:

- Determine information security and privacy requirements for the system or system service in mission and business process planning.

- Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process, and
- Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

The Contractor must allocate resources for information security and privacy and include funding for system or system service acquisition, sustainment, and supply chain-related risks throughout the SDLC.

29.3 SA-3 System Development Life Cycle (SDLC)

The Contractor must integrate the contractor information security and privacy risk management process into the SDLC, for information systems that contain IRS SBU data.

The Contractor must define and document information security and privacy roles and responsibilities throughout the SDLC. must

29.4 SA-4 Acquisition Process

Information systems containing IRS SBU data must be located and operated within the United States or its territories. Operation and maintenance of systems containing IRS SBU data must be conducted by personnel physically located within the U.S. or its territories.

The following is prohibited:

- Foreign remote maintenance
- Foreign systems monitoring
- Foreign call service centers
- Foreign help desks
- Foreign datacenters

When information systems store, process, or transmit IRS SBU, the Contractor must include security and privacy requirements and/or security and privacy specifications on all acquisition contracts used by the contractor.

Contractors must ensure before the acquisition of information system, software, hardware, professional services, maintenance, and system components that prospective suppliers are not barred from supporting/supplying US Government systems.

The Contractor must require the developer of the information system, system component, or system service to provide design and implementation information for the security controls to be employed. These include security-relevant external system interfaces, high-level design, low-level design, source code, or hardware schematics.

Properties of security controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

The Contractor must ensure that systems intended to contain IRS SBU data (i.e., beyond commercial products used as components) must be developed physically within the U.S., by U.S. citizens, or those with lawful permanent resident status.

29.5 SA-5 System Documentation

Security requirements and specifications must be included in the information system documentation. These requirements and specifications must include, but are not limited to:

- Required security capabilities.
- Development processes.
- Test and evaluation procedures.
- Required security and privacy documentation.
- Requirement's traceability.

29.6 SA-8 Security and Privacy Engineering Principles

When information systems contain IRS SBU data, the contractor must design and implement the information system using security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. Contractors must only access, maintain, or process PII that is necessary to support the IRS contract. Contractors must have processes in place to implement the principle of minimization.

Organizations apply security and privacy engineering principles primarily to newly developed information systems, or systems undergoing major upgrades. For legacy systems, organizations apply security and privacy engineering principles to system upgrades, and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems.

Security and privacy engineering principles must include, but are not limited to:

- Developing layered protections,
- Establishing sound security and privacy policy, architecture, and controls as the foundation for design,
- Incorporating security and privacy requirements into the SDLC,
- Delineating physical and logical security boundaries,
- Ensuring that system developers are trained on how to build secure software,
- Tailoring security controls to meet organizational and operational needs,
- Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk, and

- Reducing risk to acceptable levels, thus enabling informed risk management decisions.

29.7 SA-9 External System Services

The Contractor must require providers of external information system services to comply with IRS security and privacy requirements and employ IRS Publication 4812 baseline security and privacy controls. Oversight of user roles and responsibilities regarding external information system services must be defined and documented. Security and privacy control compliance by external service providers must be monitored.

29.8 SA-10 Developer Configuration Management

Contractors must require that software developers perform configuration management during software design, development, implementation, operation, and disposal. Security and privacy flaws and resolutions must be tracked and changes to software and the potential security and privacy impacts of software changes must be controlled, approved, and documented.

The software developers must create a security test and evaluation plan, implement the plan, and document the results.

29.9 SA-11 Developer Testing and Evaluation

Contractors who perform software development for the IRS must ensure that testing is conducted in a development environment.

At a minimum, the Contractor must:

- Create and implement a security test and evaluation plan and privacy assessment plan.
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.
- Document the results of the security testing/evaluation and flaw remediation processes, and
- Perform system testing and evaluation (including static and/or dynamic) throughout its life cycle that include one or more of the following:
    - Security-related functional properties,
    - Security-related externally visible interfaces,
    - High-level design,
    - Low-level design,
    - Implementation representation (source code/hardware schematics)
    - Produce evidence of the execution of the assessment plan and the results of the testing and evaluation
    - Implement a verifiable flaw remediation process
    - Correct flaws identified during security testing/evaluation.

All software custom developed or configured for the IRS must be scanned with software code vulnerability detection software before the custom software is used in support of the IRS.

29.10 SA-15 Development Process, Standards, and Tools

The Contractor must require the developer of an information system, system component, or information system service to follow a documented development process that:

- Explicitly addresses security and privacy requirements.
- Identifies the standards and tools used in the development process.
- Documents the specific tool options and tool configurations used in the development process, and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

The Contractor must review the development process, standards, tools, and tool options/configurations at a minimum annually, to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy IRS security and privacy requirements as defined by IRS Publication 4812.

29.11 SA-21 Developer Screening (C-SCRM Control)

Contractors must ensure the developer of the system, system component, or system service has appropriate access authorizations necessary for their specific assigned duties; and satisfies the personnel screening criteria (e.g., clearances, background checks, citizenship, nationality) defined in the contractor personnel security policy.

Contractors must implement screening processes for their internal developers. For system integrators who may be providing key developers that address critical components, the contractor must ensure that appropriate processes for developer screening have been used. The screening of developers should be included as a contractual requirement and be a flow-down requirement to relevant sub-level subcontractors who provide development services or who have access to the development environment.

29.12 SA-22 Unsupported System Components

Contractors including those using CSP's must replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer or provide options for alternative sources for continued support for unsupported components such as extended support agreements with the vendor.

Information system components examples include mainframes, workstations, servers (e.g., database, email, authentication, web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), OS, middleware, applications, and software versions. Support for information system components includes, but are not limited to, security patches, software updates, firmware updates, replacement parts, and maintenance contracts.

30.0 System and Communications Protection (SC)

SC ensures that information is protected from unauthorized disclosure or tampering during transit and ensures that the network communication paths where IT assets are being used to transmit IRS SBU data are protected.

30.1 SC-1 System and Communications Protection Policy and Procedures

Contractors, including those using CSP's must designate an official to manage the development, documentation, and dissemination of SC policies and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update policies and procedures annually, or if there is a significant change to SA technologies.

30.2 SC-2 Separation of System and User Functionality

Contractors including those using CSP's who manage IT development and production environments, must physically and/or logically separate user functionality from information system management functionality and the information system.

System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. Separation of system management functions from user functions includes web administrative interfaces, that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different subnets and with additional Access controls

30.3 SC-4 Information in Shared System Resources

Contractors including those using CSP's must ensure the system prevents unauthorized and unintended information transfer via shared system resources.

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that

obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

30.4 SC-5 Denial-of-Service Protection (DoS)

Contractors including those using CSP's must ensure that all IT assets and information systems are protected against and limit the effects of DoS attacks, by using boundary devices.

DoS events may be caused either by cyberattacks or by a company's failure to adequately plan for its capacity and bandwidth needs Employing increased network capacity and bandwidth combined with service redundancy reduces the susceptibility to DoS events.

30.5 SC-7 Boundary Protection

Contractors including those using CSP's must ensure that information system boundaries are controlled using managed interfaces.

The Contractor or CSP must:

- Implement subnetworks (Demilitarized Zones (DMZs)) for publicly accessible system components that are physically/ logically separated from internal contractor networks.
- Limit the number of external network connections to the information system.
- Implement a managed interface for each external telecommunication service.
    - Managed interfaces include - gateways, routers, firewalls, network-based malicious code analysis, or encrypted tunnels implemented within a security architecture.
- Establish a traffic flow policy for each managed interface.
- Filter unauthorized traffic from external networks.
    - External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include - routing, Domain Name System (DNS), and management. Unauthorized control plane traffic can occur through a technique known as "spoofing".
- Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted across each interface.
- Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
- Review exceptions to the traffic flow policy annually.
- Remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
    - Managed interfaces shall deny network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
    - Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network

communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

- The information system, in conjunction with a remote device, must prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. This is implemented within remote devices (e.g., laptop computers) through configuration settings to disable split tunneling in those devices, and in implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

Firewalls must be implemented and managed at trusted boundaries. Each trusted boundary must be monitored. Communications across each boundary must be controlled.

When employing firewalls for packet filtering, use stateful inspection firewalls or their equivalent, as opposed to stateless packet filtering firewalls or routers.

The capability must exist to conduct/perform deep packet inspection (DPI) at internet access points. This capability should be placed in line, and intrusion prevention capabilities must be utilized. Firewalls and other appropriate protection mechanisms must be employed for wireless access points.

Supplemental C-SCRM Guidance: The Contractor must implement appropriate monitoring mechanisms and processes at the boundaries between their systems and suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' systems. Provisions for boundary protections should be incorporated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. There may be multiple interfaces throughout the Contractor, supplier systems, networks, and the SDLC.

Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for supply chain components and supply chain information flow. Vulnerability, threat, and risk assessments can aid in scoping boundary protection to a relevant set of criteria and help manage associated costs. For contracts with external service providers, contractors must ensure that the provider satisfies boundary control requirements pertinent to environments and networks within their span of control. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

30.5.1 SC-7 (13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components (C-SCRM Control)

Contractors must isolate information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks, with managed interfaces to other components of the system.

30.6 SC-8 Transmission Confidentiality and Integrity

The information system must protect the confidentiality and integrity of information in transit utilizing 140-2 or later validated encryption modules. The contractor or CSP must implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, laptop computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios.

Unprotected communication paths are exposed to the possibility of interception and modification. Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and Internet Protocol Security (IPSec). Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Supplemental C-SCRM Guidance: The requirements for transmission confidentiality and integrity should be integrated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve contractor confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the contractor and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

30.7 SC-10 Network Disconnect

The information system must disconnect all network connections upon session completion, or after 30 minutes of inactivity.

Applications requiring continuous, real-time screen display (e.g., network management products, certain call center workstations as defined by company policy) must be exempt from the network inactivity disconnect threshold provided the following requirements are met:

- The logon session was not initiated by a privileged account (e.g., root in Linux/Unix, Master in Unisys).
- The inactivity exemption is documented in the appropriate operational policy approved by the CSR, and
- The workstation is in a restricted and controlled access area open only to contractors with an approved IRS clearance.

30.8 SC-12 Cryptographic Key Establishment and Management

Contractors including those using CSP's must establish and manage cryptographic keys for required cryptography employed within the information system. When public keys are used, the contractor must manage key policies and certificates.

Encryption key recovery requirements, at a minimum, must include:

- Identification of which keying material requires backup or archive for later recovery.
- The location was backed up or archived keying material must be stored.
- Responsibility assignment for protecting backed up or archived keying material.
- Required procedures for storing and recovering the keying material.
- Listing of who can request a recovery of the keying material and under what conditions.
- Listing of who will be notified when a key recovery has taken place and under what conditions, and
- Managing trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

The security role of an Encryption Recovery Agent must be assigned to support recovery processes.

Encryption products must provide for encryption key recovery to support availability needs.

Vendor-supplied default encryption keys must be changed as soon as the system or software has been installed.

30.9 SC-13 Cryptography Protection

IRS SBU data that is processed, stored, or transmitted by a contractor or CSP information system must be protected using FIPS 140-2, or later validated cryptographic modules with approved modes of operation. A list of NIST validated modules is available at the following link: http://csrc.nist.gov/groups/STM/cmvp/validation.html.

Contractor and CSP information systems must be configured to use TLS 1.2 and support TLS 1.3, if interoperability permits, TLS 1.3 is preferred. TLS must be implemented in accordance with NIST SP 800-52 Rev 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

30.10 SC-15 Collaborative Computing Devices and Applications

Collaborative devices and applications must have their remote activation capability removed/disabled. This is to prevent the device from being activated when a user is not physically present. The collaborative device must also provide an indicator to the users present that the device is active. Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. Implementation of a collaborative technology used in support of the IRS contract must be based on an assessment of risk by the contractor. Collaborative computing must not be used as a substitute for email, or other data transfer technologies.

30.11 SC-17 Public Key Infrastructure (PKI) Certificates

Contractors or CSPs who create, use, or manage PKI Certificates, the contractor must document processes with supporting procedures for digital certificate generation, installation, and distribution. The contractor must issue public key certificates under policy and/or procedure to obtain public key certificates from an approved service provider; and include only approved trust anchors in trust stores or certificate stores managed by the organization. Subscriber key pairs must be generated and stored using FIPS 140-2 or later validated modules, Security Level 2 or higher.

Private keys are protected using, at a minimum, a strong password. Refer to **Section 19.5 IA-5 Authenticator Management** for strong password requirements. A certificate must be revoked if; the associated private key is compromised, management requests revocation, or the certificate is no longer needed.

30.12 SC-18 Mobile Code

The Contractor or CSP must define acceptable, unacceptable mobile code and mobile code technologies and authorize, monitor, and control the use of mobile code within the system. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including laptop computers and smartphones.

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript.

Mobile code policy and procedures must address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Mobile code is a powerful computing tool that can introduce risks to the user's information system. Contractors, who use mobile code, must be subject to a source code review by the IRS to ensure that; there is not a potential risk of introducing malicious code into the Contractor's environment.

30.13 SC-20 Secure Name/Address Resolution Services (Authoritative Source)

The Contractor or CSP must implement Secure Name/Address Resolution Services for systems externally accessible to the organization.

Secure Name/Address Resolution Services enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A DNS server is an example of an information system that provides name/address resolution service.

Providing authoritative source information enables external clients, including remote internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include DNS servers. Additional artifacts include DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

30.14 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

The information systems must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources (e.g., DNS servers).

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNSSEC signatures or clients use authenticated channels to recursive resolvers that perform such validations.

Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

30.15 SC-22 Architecture and Provisioning for Name/Address Resolution Service

Information systems that provide name/address resolution service for an organization must be fault tolerant and implement internal/external role separation.

To eliminate single points of failure and to enhance redundancy, organizations must employ at least two authoritative domain name system servers. For role separation, DNS servers with internal roles must only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles must only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the internet).

30.16 SC-23 Session Authenticity

Contractor or CSP information systems must protect the authenticity of communication sessions by implementing TLS 1.2 or later.

Session authenticity addresses communications protection at the session level (e.g., sessions in service-oriented architectures providing web-based services) and establishes confidence at both ends of a communications session in the ongoing identities of the other parties and in the validity of information transmitted.

30.17 SC-28 Protection of Information at Rest

Contractors or CSPs storing, processing, or transmitting IRS SBU data must employ FIPS 140-2 or later validated encryption modules on their primary storage devices, servers, and storage arrays. This can be accomplished via full-disk encryption or file level-based encryption.

All digital media must employ FIPS 140-2 or later validated encryption modules, including laptops, USB storage devices, backup tapes, internal and external hard drives, etc.

Information at rest refers to the state of information when it is not being processed or is in transit and is located on system components. Such components include internal or external hard drives, storage area network devices, or databases. The focus of protecting information at rest is on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information.

Full-disk encryption is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the full-disk encryption product. Full-disk encryption restricts access before the device is booted. Once the device is booted, full-disk encryption provides no protection at all.

File encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, only it addresses individual folders instead of files. Folder/file level encryption is transparent to applications and users can provide at rest protection for data stored in the designated files and/or folders.

Supplemental C-SCRM Guidance: The Contractor must include provisions for the protection of information at rest into their agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The contractor must also ensure that they provide appropriate protections within the information systems and networks for data at rest for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC, including during requirements, development, manufacturing, test, inventory management, maintenance, and disposal. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

30.18 SC-36 Distributed Processing and Storage (C-SCRM Control)

Contractors must ensure the distribution of information processing and storage components across multiple physical and logical locations.

Processing and storage can be distributed both across the contractor's systems and networks and across the SDLC. The Contractor should ensure that these techniques are applied in both contexts.

30.19 SC-39 Process Isolation

The information system maintains a separate execution domain for each executing process. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, by implementing separate address spaces. Process isolation technologies, include sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. This capability is available in most commercial OSs that employ multi-state processor technologies.

31.0 System and Information Integrity (SI)

This section applies to contractors who are developing applications, web-based applications, and/or surveys that can be completed by a user population, and other instances where input data could be manipulated, causing inaccurate information to be generated.

31.1 SI-1 System and Information Integrity Policy and Procedures

Contractors or CSP's must designate an official to manage the development, documentation, and dissemination of SI policies and procedures for security and privacy controls.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update the policies and procedures annually, or if there is a significant change to facilitate implementing SI security controls.

31.2 SI-2 Flaw Remediation

Contractors or CSP's must implement and document a patch management process for all contractor information systems. Procedures must be established for evaluating, approving, and installing patches and hot fixes to ensure patches are installed and flaws are remediated.

Patch management is a component of CM. Patch management includes acquiring, testing, consistently applying, and monitoring patch applications within an IT infrastructure. The process of applying and certifying the application of software patches to fix flaws is critical to sustaining the desired overall security posture for enterprise-wide IT infrastructures. Timely application of patches and the management of effective implementation and oversight processes are critical to maintaining the availability of IT systems and providing desired confidentiality and data integrity.

Contractors or CSP's must identify, report, and correct information system flaws. The contractor must promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Software and firmware updates related to flaw remediation must be tested for effectiveness and potential side effects before installation. Flaws discovered during security assessments, continuous monitoring, IR activities, or information system error handling must be addressed expeditiously. The contractor must incorporate flaw remediation into their CM process. This allows for the required/anticipated remediation actions to be tracked and verified.

The Contractor must employ automated mechanisms at least monthly, to determine the state of information system components, regarding flaw remediation.

The flaw remediation process must be centrally managed.

All workstations (including laptops and mobile devices) must be appropriately reviewed for security posture prior to connection or reconnection to the network (e.g., checks for malicious code, updated virus protection software, critical software updates and patches, operating system integrity, disabled hardware).

Contractors using a CSP must ensure that they or the CSP install security-relevant software and firmware updates within the period directed by an authoritative source, or within 30 days of the update's release.

Supplemental C-SCRM Guidance: The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

31.3 SI-3 Malicious Code Protection

Malicious code protection software must be installed on all workstations, servers, virtual desktop infrastructure (VDI), and mobile computing devices. The software must perform automated scanning of all files, incoming and outgoing emails, and other network communications. The software must be configured scan IT assets at least weekly for malicious code and it must quarantine and eradicate any malicious code that is detected.

Removable media, when authorized for use including USB devices, diskettes, DVDs, or CDs, must be scanned whenever they are connected to a computing device

The Contractor or CSP must deploy malicious code protection software for the information system that include automated signature and engine updates as well as centralized management.

The Contractor or CSP must address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Malicious code protection mechanisms must be employed at information system entry and exit points, to detect and eradicate malicious code. Procedures must be defined to institute malicious code detection as a centrally managed process. In addition, the contractor must define how updates are reviewed and applied. Users of the information system must not be able to bypass malicious code protection controls implemented by the information system.

31.3.1 Email Security

Contractors must encrypt email messages and attachments that contain FTI, PII, or SBU data using FIPS 140-2 or later validated encryption modules. The Contractor must not include IRS SBU data in the subject line.

Personal email accounts are forbidden to be used to conduct business in support of the IRS contract.

Contractors must not post agency information whether using Government Furnished Equipment (GFE), company owned, or personal resources to social media, websites, or other public forums without the authority of the IRS. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government Contractor.

Electronic messaging systems (Microsoft Office, Microsoft Teams, etc.) must only be used for informal business communications and collaborations. Contractors should not use electronic messaging systems to engage in discussions regarding policy matters, business decisions, or documentation of other IRS business functions.

Contractors provisioned with GFEs, and IRS email accounts must not send e-mail messages containing IRS SBU data to non-government owned email accounts, except as required for work-related communications to members of the public or other third-parties.

When provisioned with GFE and IRS email accounts, automatic forwarding must not be used to send messages to non-IRS/Treasury email accounts. When provisioned with GFE as part of a contract, contractors must use their IRS laptop and email account for all official communications.

Contractors provisioned with GFEs, and IRS email accounts are prohibited from generating or distributing junk email, sending, or forwarding chain letters, or inappropriate messages.

Contractors provisioned with GFEs, and IRS email accounts are specifically prohibited from using GFEs for commercial purposes, in support of "for-profit" activities and ventures, and other outside employment or business activities (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

Supplemental C-SCRM Guidance: Because most of the code operated in contractor systems is not developed by the contractor, malicious code threats often originate from the supply chain. This controls applies to contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Contractors should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

31.4 SI-4 System Monitoring

Contractors including those using CSP's must employ automated tools to monitor events on the information system to: detect attacks, vulnerabilities, and to detect, deter, and report on unauthorized use of the information system.

Automated tools include host-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real-time analysis of alerts and/or notifications generated by organizational information systems.

The information system must be monitored for unauthorized local, network, and remote connections. Events and anomalies detected by intrusion monitoring tools must be analyzed. Whenever there is an elevated security level, the monitoring efforts must be increased to enable deterrence, detection, and reporting to take place, so corrective actions must be made to the networked environment. Information obtained from intrusion-monitoring tools must be protected from unauthorized access, modification, and deletion.

All contractors and CSP's must ensure they have procured and installed software to enable vulnerability detection to take place.

- The Contractor must employ automated tools and mechanisms to support near real-time analysis of events.
- The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.
- The information system provides near real-time alerts when the following indications of compromise or potential compromise occur.

All internet access points/portals must capture and retain, for at least one year, inbound and outbound traffic header information,

A host-based monitoring mechanism must be employed on information system components.

Supplemental C-SCRM Guidance: This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. SLAs with these providers should be structured to appropriately reflect this control. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

31.5 SI-5 Security Alerts, Advisories, and Directives

The Contractor or CSP must ensure that they receive information system security alerts/advisories on a regular basis, generate internal security alerts, advisories, and directives, issue alerts/advisories to appropriate contractor personnel, and take action to respond to security alerts. To avoid a Single Point of Failure, the Contractor or CSP must define appropriate personnel within the organization who must receive the alerts/advisories, and who have responsibilities to act on them.

Supplemental C-SCRM Guidance: The contractor must evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Contractors must ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Contractors must provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

31.6 SI-7 Software, Firmware, and Information Integrity

The Contractor or CSP must employ integrity verification tools to information systems, which must detect and protect against unauthorized changes to system kernels, drivers, firmware (e.g., BIOS), software (e.g., OS, applications, middleware) and security configurations.

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). State-of-the-practice integrity checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. The Contractor or CSP must document and enforce explicit rules governing the downloading and installation of software by users.

The information system must perform an integrity check of software, firmware, and information at:

- Startup or restart,
- The identification of a new threat to which the information system is susceptible,
- The occurrence of a security-relevant event,
- The installation of new hardware, software, or firmware, and
- At a minimum, annually.

The Contractor must incorporate the detection of the following into the IR capability:

- Unauthorized changes to baseline configuration setting.
- Unauthorized elevation of system privileges.

Supplemental C-SCRM Guidance: This control applies to the contractor and applicable supplier products, applications, information systems, and networks. The integrity of all applicable systems and networks should be systematically tested and verified to ensure that it remains as required so that the systems/components traversing through the supply chain are not impacted by unanticipated changes.

The integrity of systems and components should also be tested and verified. Applicable verification tools include digital signature or checksum verification; acceptance testing for

physical components; confining software to limited privilege environments, such as sandboxes; code execution in contained environments prior to use; and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer.

This control applies to contractor and applicable supplier information systems and networks. When purchasing an ICT/OT product, a contractor should perform due diligence to understand what a supplier's integrity assurance practices are. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

31.7 SI-8 Spam Protection

Contractors or CSP's must they implement a spam protection solution in their email environment. Spam Protection must be a centrally managed process and must update automatically.

31.8 SI-10 Information Input Validation

Software and applications developed by contractors or CSPs for the IRS contract must ensure that consistency checks for input validation are defined and used. This is to ensure accurate and correct inputs and prevent attacks such as cross-site scripting, application fuzzing, and buffer overflow.

31.9 SI-11 Error Handling

Software and applications developed by contractors or CSPs for the IRS contract must identify security relevant error conditions and handle them in an expeditious manner. Procedures must be developed to enable errors to be identified and corrected. Errors must not expose information to users that could utilize that information to compromise the application or information system.

31.10 SI-12 Information Management, Retention, and Information Disposal

Contractors or CSP's must manage and maintain IRS SBU data within the information system, according to record retention standards. The IRS COR must identify the record retention standards to the contractor. Contractors must minimize both security and privacy risks by disposing of IRS SBU data when it is no longer needed. The disposal or destruction of information applies to original information as well as copies and archived records, and backups including audit logs that may contain PII.

The Contractor must limit PII being processed in the information life cycle to the following elements identified within the PCLIA.

The Contractor records must maintain and manage records in accordance with approved General Records Schedule Document 12829, Records Control Schedules (RCS) Document 12990, and additional requirements defined in the contract.

The Contactor must destroy documents with IRS SBU data (including PII and tax information) by properly shredding, burning, mulching, pulping, or pulverizing beyond recognition and reconstruction. If other guidance is issued for document destruction, the Contractor must use the most stringent requirement.

The Contractor must work with the IRS COR to complete Form 11671 disposal record when records have reached their final disposition and are eligible for destruction.

In addition, once the contract expires, all data must be returned to the IRS, unless specifically identified otherwise in the contract. Records must not be maintained by the Contractor in paper or electronically, unless approved by the IRS COR.

Contractors must ensure that all IRS data and IRS-derived data are in commercially available or open and non-proprietary format for transition in accordance with the National Archives and Records Administration (NARA) disposition guidance.

NIST Special Publication 800-88, Revision 2: Guidelines for Media Sanitization, specifies the minimum required sanitization techniques to Clear, Purge, or Destroy various media and IRS SBU.

31.11 SI-16 Memory Protection

The Contractor or CSP's must implement protection on all assets used to process IRS information to protect its memory from unauthorized code execution. Security controls employed to protect memory include data execution prevention and address space layout randomization.

31.12 SI-20 Tainting (C-SCRM Control)

The Contractor has embedded data or capabilities in their development systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization.

Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may have access to the sensitive information of a contractor and IRS SBU.

32.0 Supply Chain Risk Management (SR)

Supply Chain Risk Management (SCRM) ensures that contractors reliance on systems and services from vendors as well as the nature of the relationships with those providers are identified. SCRM activities include identifying and assessing SR risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans.

32.1 SR-1 Supply Chain Risk Management Policy and Procedures

Contractors must designate an official to manage the development, documentation, and dissemination of the SR policies and procedures.

The policies and procedures must address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among Organization Entities
- Compliance

The Contractor must review/update the SR policies and procedures annually, or if there is a significant change.

32.2 SR-2 Supply Chain Risk Management Plan

Contractors must establish and implement a SCRM plan for managing SR risks associated with the design, acquisition, delivery, integration, operations, maintenance, and disposal of information systems used in support of the IRS contract. A supply chain risk management team must be established to lead and support SCRM activities.

Contractors must review/update the SCRM plan annually, or if there is a significant change.

The SCRM plan must addresses management, implementation, and monitoring of SR controls and the development/sustainment of systems across the SDLC.

SCRM plans must include an expression of the SR risk tolerance for the organization, acceptable SR risk mitigation strategies, a process for consistently evaluating and monitoring SR risk, approaches for implementing and communicating the plan, a description of and justification for SCRM measures taken, and associated roles and responsibilities.

SCRM plans must address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the

security design principles implemented as part of the SDLC systems security engineering processes.

32.3 SR-3 Supply Chain Controls and Processes

The Contractor must implement SR elements and processes in their SCRM Plan.

SR elements include controls or tools employed for the following:

- Research and development
- Design
- Manufacturing
- Acquisition
- Delivery
- Integration
- Operations and maintenance
- Disposal of systems and system components

Supply chain processes include the following:

- Hardware, software, and firmware development processes,
- Shipping and handling procedures,
- Personnel security and physical security programs,
- Configuration management tools,
- Techniques, and
- Procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

The Contractor must develop and implement a process to identify and address weaknesses or deficiencies in their SR controls and processes.

The Contractor must employ controls and processes to protect against SR risks to the information system, system components, or system services, and to limit the harm or consequences from supply chain-related events.

The Contractor must document the selected and implemented supply chain processes and controls in the supply chain risk management plan.

32.4 SR-5 Acquisition Strategies, Tools, and Methods

The Contractor must develop and implement acquisition strategies and methods to protect against, identify, and mitigate SR risks.

The Contractor must provide awareness training to employees about SR risk and available mitigation strategies.

The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the contractor's environment. Tools and techniques may provide protection against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the SDLC.

32.5 SR-6 Supplier Assessments and Reviews

The Contractor must annually assess and review the supply chain-related risks associated with suppliers and the information system, system components, or system services provided.

An assessment and review of supplier risk includes security and SCRM processes, foreign ownership control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers.

The supplier reviews may be conducted by the organization or by an independent third-party. Supplier reviews must consider; documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits.

32.6 SR-8 Notification Agreements

The Contractor and must notify the IRS COR and CSIRC Incident Response Operations Team at (240) 613-3606/ or CSIRC@irs.gov which is available 24x7x365, immediately upon discovery of a potential Supply Chain Attack/Compromise that effects an information system and/or system component that supports the IRS contract. Within one hour of notification of a possible Supply Chain Attack/Compromise, the COR must notify the CSA team @ it.cyber.csa.request@irs.gov.

The Contractor must ensure that agreements and procedures are established with entities involved in the SR for the system, system components, or system services for notification of SR compromises and results of assessments or audits.

The establishment of agreements and procedures facilitates communications among SR entities. Early notification of compromises and potential compromises in the SR that can potentially adversely affect or have adversely affected information systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the SR entity resolve a concern or improve its processes.

32.7 SR-10 Inspection of Systems or Components

The Contractor must inspect information systems or system components when removed from contractor-controlled areas or when there may have been a potential security incident.

The inspection of systems or system components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from contractor-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Supplemental C-SCRM Guidance: Contractors must inspect critical systems and components, at a minimum, for assurance that tamper resistance controls are in place and to examine whether there is evidence of tampering. Products or components must be inspected prior to use and periodically thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Contractors must require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors and flow down to subcontractors, when relevant.

32.8 SR-11 Component Authenticity

The Contractor must implement an anti-counterfeit policy and procedure that includes a process to detect and prevent counterfeit components from entering the information system. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

The Contractor must train personnel with relevant roles to detect counterfeit system components including hardware, software, and firmware. Sources of counterfeit components include manufacturers, developers, vendors, and counterfeit websites.

The Contractor must maintain configuration control over the system components awaiting service or repair and serviced or repaired components awaiting return to service.

32.9 SR-12 Component Disposal

The Contractor must dispose of software code, documentation, tools, or system components using IRS approved methods. Software code, documentation, tools, or system components can be disposed of at any time during the SDLC (not only in the disposal or retirement phase of the life cycle).

Disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, and partial reuse of components. Opportunities for compromise during disposal affect

physical and logical data including system documentation, portable media with software code; or routers or servers that include permanent storage which contain IRS SBU data.

33.0 Privacy

Agencies and the contractors acting on their behalf must abide by NIST SP 800-53 Rev. 5. All privacy controls are initially assessed in the PCLIA and subsequently through contractor onsite or virtual visits.

In addition to the privacy controls in this publication, IRM 10.5.1 outlines the IRS Privacy Principles and establishes the minimum baseline privacy policy and requirements for all IRS SBU data (including PII and FTI) to:

- Establish and maintain a comprehensive privacy program,
- Comply with privacy requirements and manage privacy risks,
- Ensure the protection and proper use of SBU data of the IRS,
- Prevent unauthorized access to SBU data of the IRS, and
- Enable operation of IRS environments and business units that meet the requirements of this policy and support the business needs of the organization.

Publicly available sections of IRM 10.5.1 apply to the contractor (included under the term "IRS personnel") and are available at:
(https://www.irs.gov/irm/part10/irm_10-005-001)

34.0 Termination of Contract

At the end of the contract period, or if the contract is terminated within the contract period, the contractor must coordinate with the IRS to ensure contractor and contractor employee access privileges to IRS information, IRS systems, and facilities are revoked in a timely manner, as necessary.

A completed Form 14604, Contractor Separation Checklist is required. This checklist is used to separate a contractor from an IRS contract, and to document the return of all security items, Government property, and information/records to the appropriate office.

Contractors must confirm to IRS officials that information furnished under the contract has been properly returned, disposed of, or destroyed. This includes assuring the IRS that all IT assets, including laptops, information systems, servers, routers, printers, faxes, switches, voice recordings, and all removable and fixed media have been sanitized of all IRS information prior to returning into production for other use.

Contractors required to return IRS information and property (as a part of the contract requirements) must use a process that ensures that the confidentiality of the SBU data is always protected during transport.

A log must be maintained to ensure that all media destroyed has been identified by the date of destruction, content of media, serial number, type of media (CD, DVD), etc.) destruction performed, personnel performing destruction, and witness.

All VoIP must be sanitized prior to returning to production, when SBU data is stored on these devices.

All hard drives and removable media must be inventoried, sanitized, and logged to demonstrate data destruction for all IT assets used to handle SBU data.

All hard copies must be returned using double-wrapped envelopes and traceable mail.

34.1 Destruction or Return of SBU Data

When the contract is officially closed out, SBU data provided to the contractor or created by the contractor must be returned to the IRS or destroyed as directed in writing by the IRS. This includes copies of reports, extra copies, photo impressions, information system printouts, carbon paper, notes, stenographic notes, and work papers.

See **Section 22.6 MP-6 Media Sanitization**, concerning media sanitation and **Section 30.10 SI-12 Information Management, Retention, and Information Disposal**, concerning the transfer of data to the IRS.

Contractors must follow the IRS RCS, Document 12990 and General Records Schedules (GRS), Document 12829 for NARA approved records retention and destruction authorization

applicable to their IRS business use. The contract owner must have the records retention schedules available and incorporated into the contract.

Destruction of media is the ultimate form of sanitization. After the destruction of the media, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, cross-cut shredding, incinerating, pulverizing, and melting.

Either an IRS employee or a contractor with IRS approved interim/final staff-like access must be present during the incineration and/or destruction of SBU data. The employee must be present and observe the destruction process.

35.0 Taxpayer Browsing Protection Act of 1997 and Unauthorized Access and Disclosures

The Taxpayer Browsing Protection Act of 1997 covers the willful unauthorized access or inspection of any taxpayer records, (the IRS calls this UNAX) including hard copies of returns and return information as well as returns maintained on an information system. **Unauthorized access or inspection of taxpayer records is a misdemeanor**.

This crime is punishable by fines and could also result in prison terms. The provisions and applicable criminal penalties under the Taxpayer Browsing Protection Act of 1997 apply to all contractors, and contractor employees. Before any contractor employee can be given access to returns, they must have been approved for interim/final staff-like access by IRS PS and certify that they have been provided UNAX training.

Once contractors have taken IRS required training, completion documentation must be returned to the Contractor Security Management Office, and to the COR or designee. UNAX forms must not be retained at the contractor site.

UNAX deals with the unauthorized access. UNAX also addresses any inadvertent access (accidental) made by an employee or a contractor.

Contractors must ensure that no tax return information is disclosed to any person not authorized to access the information. IRC Section 7213 covers unauthorized disclosure of information. Unauthorized disclosure of tax return information is a felony.

As part of the certification, and at least annually afterwards, contractor employees must be advised of the provisions of IRC Sections 7213, 7213A, and 7431 (See Section 36.0 Exhibit 1 - Legal Requirements and Section 37.0 Exhibit 2 - Taxpayer Browsing Protection Act).

Contractors must make their employees aware that disclosure restrictions and the penalties apply even after employment with the contractor has ended.

It shall be certified that contractor employees understand security policy and procedures requiring their awareness and compliance.

36.0 Exhibit 1 - Legal Requirements

36.1 IRC Section 7213 - Unauthorized Disclosure of Information

36.1.1 Federal Employees

It shall be unlawful for any officer or employee of the United States, or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. **Any violation of this paragraph shall be a felony** punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than five years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

36.1.2 Other Persons

It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in a manner not authorized by this title thereafter to willfully print or publish in any manner not provided by law any such return or return information. **Any violation of this paragraph shall be a felony** punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than five years, or both, together with the cost of prosecution.

36.1.3 Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive because of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than five years, or both, together with the cost of prosecution.

36.2 Section 7213A - Unauthorized Inspection of Returns or Return Information

36.2.1 Federal Employees and Other Persons

It shall be unlawful for (A) any officer or employee of the United States, or (B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than one year, or both, together with the costs of prosecution.

For purposes of this section, the terms "inspect", "return", and "return information" have respective meanings given such terms by section 6103(b).

37.0 Exhibit 2 - Taxpayer Browsing Protection Act

37.1 IRC Section 7431 - Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information.

37.1.1 Inspection or Disclosure by a Person Who is Not an Employee of the United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

37.1.2 Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of

(1) The greater of-

A. $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

B. The sum of:

i. the actual damages sustained by the plaintiff because of such unauthorized inspection or disclosure plus,
ii. in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages plus,

(2) The cost of the action.

(3) Subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

37.1.3 Definitions

For purposes of this section, the terms "inspect", "inspection", "return" and "return information" have the respective meanings given such terms by section 6103(b).

Appendix A: Acronyms

Acronym	Acronym Description
AC	Access Control
AI	Artificial Intelligence
AT	Awareness Training
AU	Audit and Accountability
ATM	Automated Teller Machine
BOD	Business Operating Division
VSS	Video Surveillance Systems
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc - Read Only Memory
CD-RW	Compact Disc - Rewritable
CM	Configuration Management
CO	Contracting Officer
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf Software
CP	Contingency Planning
CSA	Contractor Security Assessment
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
DM	Data Minimization and Retention
DVD	Digital Video Device
FAR	Federal Acquisition Regulation
FDE	Full-Disk Encryption
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act 2002. Amended 2014

Acronym	Acronym Description
FMSS	Facilities Management and Security Services
FTC	Federal Trade Commission
FTI	Federal Tax Information
FTP	File Transfer Protocol
GLB	Gramm-Leach Bliley
GRS	General Records Schedules
GSA	General Services Administration
HIDS	Host-Based Intrusion Detection System
IA	Identification & Authentication
IDS	Intrusion Detection Systems
IP	Internet Protocol
IR	Incident Response
IRC	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
LAN	Local Area Network
LES	Law Enforcement Sensitive
MA	Maintenance
MAC	Media Access Control
MP	Media Protection
NARA	National Archives and Records Administration
NAT	Network Address Translation
NET	Networked Information Technology
NIDS	Network-Based Intrusion Detection System
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OMB	Office of Management & Budget
PCLIA	Privacy and Civil Liberties Impact Assessment
PE	Physical & Environmental Protection
PED	Personal Electronic Device

Acronym	Acronym Description
PGLD	Privacy, Governmental Liaison and Disclosure
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PS	Personnel Security
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RAC	Risk Assessment Checklist
RCS	Records Control Schedules
RIM	Records and Information Management
ROM	Read Only Memory
RPO	Recovery Point Objective
RTO	Recover Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment & Authorization
SAMC	Situational Awareness Management Center
SBU	Sensitive But Unclassified
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SI	System and Information Integrity
SOFT	Software Application Development or Maintenance
SP	Special Publication
SQL	Structured Query Language
SR	Supply Chain Risk Management
SSP	System Security Plan
TCP	Transmission Control Protocol
UNAX	Unauthorized Access
USB	Universal Serial Bus
USC	United States Code
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Networks

Appendix B: Glossary

A

Access Control: The process of granting or denying specific requests to: 1) obtain and use information and related information processing services, and 2) enter specific physical facilities (e.g., Contractor Facilities).

Account Manager: User account management involves the process of requesting, establishing, issuing, modifying, and closing user accounts; tracking users and their access authorization and privileges.

Accountability: A process of holding users responsible for actions performed on an information system.

Adequate Security: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Alternate Work Site: Any working area that is attached to the WAN either through a Public Switched Data Network (PSDN) or through the Internet.

Assurance: A measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Audit: An independent examination of security controls associated with a representative subset of contractor IT assets to determine the operating effectiveness of information system controls; ensure compliance with established policy and operational procedures; and recommend changes in controls, policy, or procedures where needed.

Audit Trail: A chronological record of information system activities sufficient to enable the reconstruction, reviewing and examination of security events related to an operation, procedure, or event in a transaction, from its inception to results.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. See Identification.

Authenticator: The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authorization: Access privileges granted to a user, program, or process.

Availability: Timely, reliable access to information and information services for authorized users.

B

Banner: Display of an information system outlining the parameters for information system or information use.

Baseline Security Requirements: A description of the minimum-security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) a person accesses or potentially accesses personally identifiable information for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions).

C

Classified Information: National security information classified pursuant to Executive Order 12958.

Cloud Service Provider: A cloud service provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals.

Compromise: The disclosure of sensitive information to persons not authorized to receive such information.

Confidentiality: Preserving authorized restrictions on information access and disclosure.

Configuration Management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the information system development life cycle.

Continuous Monitoring: Maintaining an ongoing awareness to support organizational risk decisions.

Contingency Plan: Management policy and procedures used to guide a contractor response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the contractor to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Contracting Officer: means an individual, designated, and authorized responsible for managing contracts/acquisitions and overseeing their implementation.

Contracting Officer's Representative: As defined in FAR Part 2, the COR means an individual, designated, and authorized in writing by the CO to perform specific technical or administrative functions.

Contractor Security Assessments: Contractor Security Assessments are evaluations performed by the IRS to assess and validate the effectiveness of security & privacy controls established to protect IRS information and information systems.

COTS: Commercial off the shelf

Counter Measures: Actions, devices, procedures, mechanisms, techniques, or other measures that reduce the vulnerability of an information system.

Cryptography: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

CSIRC: Computer Security Incident Response Center

D

Data: A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

Data At Rest: All data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media, etc.) while excluding data that is traversing in a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Disaster Recovery Plan: A written plan for recovering one or more systems at an alternate facility in response to a major hardware or software failure or destruction of facilities

Decryption: The process of converting encrypted information into a readable form. This is also called deciphering.

De-militarized Zone: Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Denial of Service: The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Digital Certificate: A digital representation of information used in conjunction with a public key encryption system, which at a minimum: 1) Identifies the certification authority issuing it; 2) Names or identifies its subscriber; 3) Contains the subscriber's public key; 4) Identifies its operational period. 5) Is digitally signed by the certification authority issuing it.

Disclosure: The making known to any person in any manner whatever a return or return information. See IRC 26 U.S.C. § 6103(b)(8) for the statutory definition of disclosure.

Discretionary Access Control: A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need to know of users, groups, or processes.

Domain Name System: A hierarchical naming system that retains artifacts related to the lookup, including cryptographic keys, DNS resource records, etc.

E

Encryption: Conversion of plaintext to ciphertext using a cryptographic algorithm.

Encryption Algorithm: A formula used to convert information into an unreadable format.

External Information System: Information systems or components of information systems that are outside of the authorization boundary established by the contractor and for which the contractor typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

External Network: Any network residing outside the security perimeter established by the telecommunications information system.

Extranet: A private data network using the public telephone network to establish a secure communications medium among authorized users (e.g., contractor, vendors, business partners). An extranet extends a private network (often referred to as an intranet) to external parties in cases where both parties may be benefit from exchanging information quickly and privately.

F

Federal Tax Information: Any return or return information received from the IRS or secondary source, such as SSA etc. FTI includes any information created by the recipient that is derived from return or return information. (Internal Revenue Code (IRC) § 6103, confidentiality and disclosure of returns and return information).

File Permissions: A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

File Server: A local area network information system dedicated to providing files and data storage to other network stations.

Firewall: Telecommunication device used to regulate logical access authorities between network information systems.

Firmware: Microcode programming instructions permanently embedded into the Read Only Memory (ROM) control block of an information system. Firmware is a machine component of information system, like an information system circuit component.

FMSS: Facilities Management and Security Services

G

General Support System: An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

H

HOST: An information system dedicated to providing services to many users. Examples of such information systems include mainframes, mini-information systems or servers providing Dynamic Host Configuration Protocol (DHCP) services.

I

Information Assurance: Measures that protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.

Identification: A mechanism used to request access to information system resources by providing a recognizable unique form of identification such as a login-id, user-id, or token. Also, see Authentication.

Incident: An occurrence that one, actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or a system; or two, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's systems.

Interconnection Security Agreement: An agreement established between organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

Information System: A collection of hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control.

Information System Security: The protection of information systems and information against unauthorized access, use modification or disclosure – ensuring confidentiality, integrity and availability of information systems and information.

Integrity: Protection of information systems and information from unauthorized modification; ensuring quality, accuracy, completeness, non-repudiation, and authenticity of information.

Intranet: A private network using TCP/IP, the Internet, and world-wide-web technologies to share information quickly and privately between authorized user communities, including contractors, vendors, and business partners.

K

Key: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

Least Privilege: A security principle stating users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

Major Application: An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. **Note**: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and must be treated as major. Adequate security for other applications must be provided by security of the information systems in which they operate.

Malicious Code: Rogue information system programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity and availability of information systems and information.

Mass Storage Device: A storage drive: hard disk, solid state disk, or USB drive that makes it possible to store and port large amounts of data across computers, servers and within an IT environment.

Media: There are two primary types of media in common use: hard copy media are physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. Electronic (i.e., "soft copy") are devices containing bits and bytes such as hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices.

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Mobile Code: Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Multi-factor Authentication: Requires using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (i.e., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

N

Network: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected information systems. Examples of networks include local area networks, wide area networks, metropolitan area networks and wireless area networks.

NIST: National Institute of Standards and Technology

Non-Repudiation: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets. That is, senders and recipients of information cannot deny their actions.

O

Object Reuse: The reassignment of storage medium, containing residual information, to potentially unauthorized users or processes.

P

Packet: A unit of information traversing a network.

Password: A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

Penetration Testing: A testing method where security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

Personally Identifiable Information: Per OMB Circular A-130: "Personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual".

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency *(in this case, the contractor on behalf of the IRS)* shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it

is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.
Circular A-130, page 33:

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

PGLD: Privacy, Governmental Liaison and Disclosure.

Plan of Actions and Milestones: A management tool used to assist contractors in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems, as defined in OMB Memorandum 02-01.

Potential Impact: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on contractor operations, contractor assets, or individuals.

Protocol: A set of rules and standards governing the communication process between two or more network entities.

Privacy and Civil Liberties Impact Assessment: A PCLIA is a process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form about members of the public and agency employees. The PCLIA also identifies and evaluates protections to mitigate the impact to privacy of collecting such information.

Privileged Account: An account with elevated privileges.

Privacy Threshold Analysis: An abbreviated analysis used to identify and document any additional privacy compliance requirements and can be used to determine whether a full PCLIA is needed.

Public Key Infrastructure: is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

R

Recovery Point Objective: The point in time to which data must be recovered after an outage.

Recovery Time Objective: The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business process.

Remnants: Residual information remaining on storage media after reallocation or reassignment of such storage media to different contractors, organizational elements, users, or processes. See Object Reuse.

Remote Maintenance: Maintenance activities conducted by individuals communicating external to a system security perimeter.

Removable Media: Any type of storage device that can be removed from a computer while the system is still running. Examples include CDs, DVDs, diskettes, and USB drives.

Residual Risk: Portions of risk remaining after security controls or countermeasures are applied.

Returns and Return Information: Any information defined by IRC, 26 U.S.C. § 6103(b). Tax information from IRS business processes come under many names, such as FTI, IRC § 6103-protected information, taxpayer data, taxpayer information, tax return information, return information, case information, SBU data, and PII. See FTI.

Risk: The potential adverse impact to the operation of information systems affected by threat occurrences on contractor operations, assets, and people.

Risk Assessment: The process of analyzing threats to and vulnerabilities of an information system to determining the potential magnitude of harm and identifying cost effective countermeasures to mitigate the impact of such threats and vulnerabilities.

Risk Level: The security impact risk level is the low, moderate, or high impact level assigned to an information system in accordance with FIPS 199 and FIPS 200 based on the types of information processed, stored and/or transmitted by the information system.

Risk Management: The routine process of identifying, analyzing, isolating, controlling, and minimizing security risk to achieve and maintain an acceptable risk level. A risk assessment is an instrumental component of the risk management life cycle.

S

Safeguards: Protective measures prescribed to enforce the security requirements specified for an information system. This is synonymous with security controls and countermeasures.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

SCADA: Supervisory Control and Data Acquisition.

Security Content Automation Protocol: A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

Security Information and Event Management: A tool/application that provides the ability to gather security data from system components and present that data as actionable information via a single interface.

Security Policy: The set of laws, rules, directives, and practices governing how contractors protect information systems and information.

Security Requirement: The description of a specification necessary to enforce the security policy. See Baseline Security Requirements.

Sensitive But Unclassified: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act of 1974), but which has not been specifically authorized under criteria established by an Executive Order or Congress to be kept secret in the interest or national defense for foreign policy.

Service Level Agreement: Defines the specific responsibilities of the service provider and sets the customer expectations.

Significant Change: Also referred to as major change – A change that is likely to affect the security state of a system.

Staff-Like Access: Staff-Like Access is the authority granted to perform one or more of the following:

- Enter IRS facilities or space (owned or leased) unescorted (when properly badged),
- Possess login credentials to information systems (IRS or vendor-owned systems that store, collect, and/or process IRS information),
- Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) Sensitive but Unclassified (SBU) data, wherever the location,
- Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room, wherever the location. These items include, but are not limited to security devices/records, computer equipment, Identification media, and
- Enter physical areas, wherever the location, that store/process SBU data (unescorted).

Staff-Like Access is granted to an individual who is not an IRS employee (and includes, but is not limited to: contractors/subcontractors, whether procured by IRS or another federal agency, vendors, courier and printing services, outside experts, consultants, paid/unpaid interns, sign language interpreters, document recovery services, other federal employees, delivery services, cleaning/maintenance employees, etc.), and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS PS.

Suitability: A person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development, acquisition, implementation, operation, and maintenance; with ultimately its disposal that instigates another system initiation.

System Security Plan: An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

T

Threat: An activity, event, or circumstance with the potential for causing harm to information system resources.

Trusted Network: The networks inside an organization's security perimeter.

U

User: A person or process authorized to access an information system.

User Identifier: A unique string of characters used by an information system to identify a user or process for authentication.

V

Vendor Point of Contact: The POC is the contractor's primary point of contact for the Government on all security-related matters and the person responsible for ensuring the security of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls.

Virus: A self-replicating, malicious program that attaches itself to executable programs.

Virtual Private Network: A virtual network, built on top of existing physical networks that provide a secure communications tunnel for data and other information transmitted between networks.

Vulnerability: A known deficiency in an information system that threat agents can exploit to gain unauthorized access to sensitive or classified information.

Vulnerability Assessment: Systematic examination of an information system to determine its' security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

Vulnerability Scan: A scan of the network environment, less invasive than a penetration test that can be used to identify information system vulnerabilities to a contractor's management.

W

Whitelist: A list of hosts or applications that are known to be benign and are approved for use within an organization and/or system.

X

Y

Z

Appendix C: Security Control Levels

All contractors are required to use the applicable Security Control Levels to ensure the protection of IRS SBU data and information systems, including contracting actions using simplified acquisition procedures. When additional controls are required, these must be defined in the solicitation/contract. If a security control level other than what is described here, or in Figure 1 or in applicable clauses to the contract as the norm or default level is to be used, then that security control level will be identified in the contract.

Figure 1 – Security Control Level High Water Mark of this appendix serves as a quick reference guide on the conditions and operators typical for each security control level within a hierarchy.

Table 5 – Table of Security Controls identifies the specific security controls applicable to each security control level.

Legend

The "high water" mark concept employs a hierarchy that goes from the least stringent security control. It considers several risk-based factors with due deference to higher risk factors (operators) such as networked environments and software development).

Figure 1 Security Control Level High Water Mark

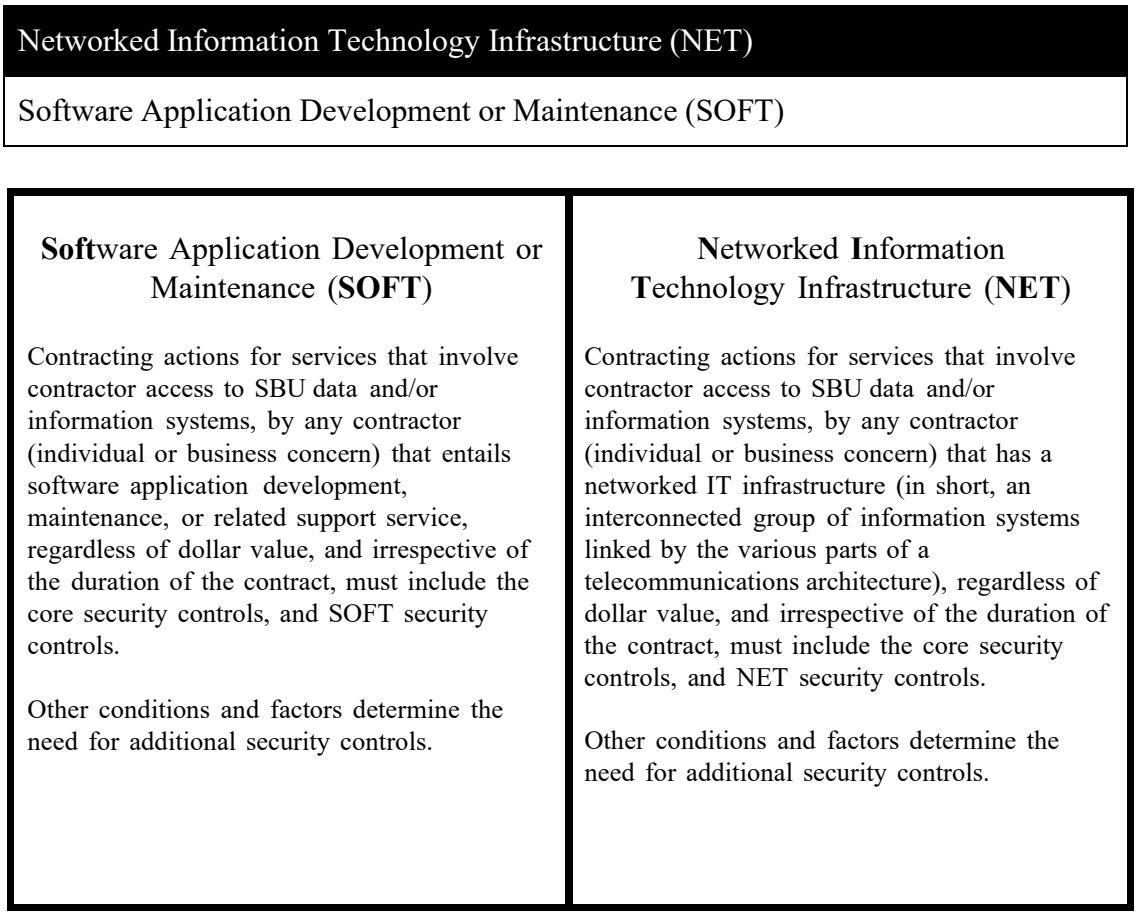

Table 5: Security Controls Table

NIST CONTROL	Networked Information Technology Infrastructure (NET)	Software Application Development or Maintenance (SOFT)	Cyber Security Supply Chain Risk Management (C SCRM)	Privacy, Governmental Liaison and Disclosure (PGLD Privacy)
AC-1 Access Control Policy and Procedures	X	X	X	X
AC-2 Account Management	X	X	X	
AC-3 Access Enforcement	X	X	X	X
AC-4 Information Flow Enforcement	X	X	X	
AC-5 Separation of Duties	X	X	X	
AC-6 Least Privilege	X	X		
AC-7 Unsuccessful Login Attempts	X	X		
AC-8 System Use Notification	X	X		
AC-11 Device Lock	X	X		
AC-12 Session Termination	X	X		
AC-14 Permitted Actions without Identification or Authentication	X	X		
AC-17 Remote Access	X	X	X	
AC-18 Wireless Access	X	X		
AC-19 Access Control for Mobile Devices	X	X		
AC-20 Use of External Systems	X	X	X	
AC-21 Information Sharing	X	X		X
AC-22 Publicly Accessible Content	X	X		X
AC-22 Data Mining			X	
AT-1 Awareness and Training Policy and Procedure	X	X		X
AT-2 Literacy Training and Awareness	X	X		X
AT-3 Role Based Training	X	X	X	

AT-4 Training Records	X	X		X
AU-1 Audit and Accountability Policy and Procedures	X	X		X
AU-2 Event Logging	X	X	X	X
AU-3 Content of Audit Records	X	X	X	X
AU-4 Audit Log Storage Capacity	X	X		
AU-5 Response to Audit Logging Processing Failures	X	X		
AU-6 Audit Record Review, Analysis, and Reporting	X	X		
AU-7 Audit Record Reduction and Report Generation	X	X		
AU-8 Time Stamps	X	X		
AU-9 Protection of Audit Information	X	X		
AU-11 Audit Record Retention	X	X		X
AU-12 Audit Record Generation	X	X	X	
AU-13 Monitoring for Information Disclosure			X	
AU-14 Session Audit			X	
AU-16 (2) Cross-Organizational Audit Logging | Sharing of Audit Information			X	
CA-1 Assessment, Authorization, and Monitoring Policies and Procedures		X		X
CA-2 Control Assessments		X		X
CA-3 Information Exchange	X	X	X	
CA-5 Plan of Action and Milestones	X	X		X
CA-6 Authorization	X	X		X
CA-7 Continuous Monitoring	X	X		X
CA-8 Penetration Testing	X	X		
CA-9 Internal System Connections	X	X		

CM-1 Configuration Management Policy and Procedures	X	X		X
CM-2 Baseline Configuration	X	X	X	
CM-3 Configuration Change Control	X	X	X	
CM-4 Impact Analysis	X	X		X
CM-5 Access Restrictions for Change	X	X		
CM-6 Configuration Settings	X	X	X	
CM-7 Least Functionality	X	X	X	
CM-8-System Component Inventory	X	X	X	
CM-9 Configuration Management Plan	X	X	X	
CM-10 Software Usage Restrictions	X	X		
CM-11 User-Installed Software	X	X		
CM-12 Information Location	X	X		
CP-1 Contingency Planning Policy and Procedures	X	X		
CP-2 Contingency Plan	X	X		
CP-2 (7) Contingency Plan | Coordinate with External Service Providers			X	
CP-3 Contingency Training	X	X	X	
CP-4 Contingency Plan Testing	X	X		
CP-6 Alternate Storage Site	X	X		
CP-7 Alternate Processing Site	X	X		
CP-8 Telecommunications Services	X	X		
CP-9 System Backup	X	X		

CP-10 System Recovery and Reconstitution	X	X		
IA-1 Identification and Authentication Policy and Procedures	X	X		
IA-2 Identification and Authentication (Organizational Users)	X	X	X	
IA-3 Device Identification and Authentication	X	X		
IA-4 Identifier Management	X	X	X	
IA-5 Authenticator Management	X	X	X	
IA-6 Authenticator Feedback	X	X		
IA-7 Cryptographic Module Authentication	X	X		
IA-8 Identification and Authentication (Non-Organizational Users)	X	X		
IA-9 Service Identification and Authentication			X	
IR-1 Incident Response Policy and Procedures	X	X	X	X
IR-2 Incident Response Training	X	X	X	X
IR-3 Incident Response Testing	X	X		X
IR-4 Incident Handling	X	X		X
IR-4 (10) Incident Handling | Supply Chain Coordination			X	
IR-5 Incident Monitoring	X	X		X
IR-6 Incident Reporting	X	X		X
IR-6 (3) Incident Reporting | Supply Chain Coordination			X	
IR-7 Incident Response Assistance	X	X		X
IR-7 (2) Incident Response Assistance | Coordination and External Providers			X	

IR-8 Incident Response Plan	X	X	X	X
IR-9 Information Spillage Response			X	
MA-1 Maintenance Policy and Procedures	X	X	X	
MA-2 Controlled Maintenance	X	X		
MA-3 Maintenance Tools	X	X		
MA-4 Non-Local Maintenance	X	X	X	
MA-5 Maintenance Personnel	X	X		
MA-6 Timely Maintenance	X	X		
MP-1 Media Protection Policy and Procedures	X	X		X
MP-2 Media Access	X	X		
MP-3 Media Marking	X	X		
MP-4 Media Storage	X	X	X	
MP-5 Media Transport	X	X		
MP-6 Media Sanitization	X	X	X	X
MP-7 Media Use	X	X		
PE-1 Physical and Environmental Protection	X	X		X
PE-2 Physical Access Authorizations	X	X	X	
PE-3 Physical Access Control	X	X		
PE-4 Access Control for Transmission Medium	X	X		
PE-5 Access Control for Output Devices	X	X		
PE-6 Monitoring Physical Access	X	X		
PE-8 Visitor Access Records	X	X		X
PE-9 Power Equipment and Power Cabling	X	X		
PE-10 Emergency Shutoff	X	X		
PE-11 Emergency Power	X	X		

PE-12 Emergency Lighting	X	X		
PE-13 Fire Protection	X	X		
PE-14 Environmental Controls	X	X		
PE-15 Water Damage Protection	X	X		
PE-16 Delivery and Removal	X	X		
PE-17 Alternate Work Site	X	X		
PE-23 Facility Location			X	
PL-1 Planning Policy and Procedures	X	X		X
PL-2 System Security and Privacy Plans	X	X	X	X
PL-4 Rules of Behavior	X	X		X
PL-8 Security and Privacy Architectures	X	X		X
PM-5 Inventory of Personally Identifiable Information	X	X	X	X
PM-18 Privacy Program Plan	X	X	X	X
PM-19 Privacy Program Leadership Role	X	X		X
PM-20 Dissemination of Privacy Program Information	X	X		X
PM-25 Minimization of PII used in testing, training, research	X	X		X
PM-26 Complaint Management	X	X		X
PS-1 Personnel Security Policy and Procedures	X	X	X	X
PS-2 Position Categorization	X	X		X
PS-3 Personnel Screening	X	X	X	
PS-4 Personnel Termination	X	X		X
PS-5 Personnel Transfer	X	X		X

PS-6 Access Agreements	X	X	X	X
PS-7 External Personnel Security	X	X		
PS-8 Personnel Sanctions	X	X		
PT-1 PII Policy and Procedures	X	X	X	X
PT-2 Authority to Process PII	X	X		X
PT-3 PII Processing Purposes	X	X		X
PT-5 Privacy Notice	X	X		X
PT-7 PII - Social Security Numbers	X	X		X
RA-1 Risk Assessment Policy & Procedures	X	X		X
RA-2 Security Categorization	X	X		
RA-3 Risk Assessment	X	X		X
RA-5 Vulnerability Monitoring and Scanning	X	X	X	
RA-8 Risk Assessment – Privacy Impact Assessments				X
RA-9 Criticality Analysis			X	
SA-1 System and Security Acquisition Policy and Procedures	X	X		X
SA-2 Allocation of Resources	X	X		X
SA-3 System Development Life Cycle	X	X		X
SA-4 Acquisition Process	X	X		X
SA-5 System Documentation		X		
SA-8 Security and Privacy Engineering Principles		X		X
SA-9 External System Services	X	X		X
SA-10 Developer Configuration Management		X		
SA-11 Developer Testing and Evaluation		X		X

SA-15 Development Process, Standards, and Tools		X		
SA-21 Developer Screening			X	
SA-22 Unsupported System Components	X	X		
SC-1 System and Communications Protection Policy and Procedures	X	X		
SC-2 Separation of System and User Functionality	X	X		
SC-4 Information in System Shared Resources		X		
SC-5 Denial of Service Protection	X	X		
SC-7 Boundary Protection	X	X	X	
SC-7 (13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components			X	
SC-8 Transmission Confidentiality and Integrity	X	X	X	
SC-10 Network Disconnect	X	X		
SC-12 Cryptographic Key Establishment and Management	X	X		
SC-13 Cryptography Protection	X	X		
SC-15 Collaborative Computing Devices and Applications		X		
SC-17 Public Key Infrastructure Certificates	X	X		
SC-18 Mobile Code		X		
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	X	X		
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	X	X		

SC-22 Architecture & Provisioning for Name/Address Resolution Service	X	X		
SC-23 Session Authenticity	X	X		
SC-28 Protection of Information at Rest	X	X	X	
SC-36 Distributed Processing and Storage			X	
SC-39 Process Isolation		X		
SI-1 System and Information Integrity Policy and Procedures	X	X		X
SI-2 Flaw Remediation		X	X	
SI-3 Malicious Code Protection	X	X	X	
SI-4 System Monitoring	X	X	X	
SI-5 Security Alerts, Advisories, and Directives	X	X	X	
SI-7 Software Firmware, and Information Integrity		X	X	
SI-8 Spam Protection	X	X		
SI-10 Information Input Validation		X		
SI-11 Error Handling		X		
SI-12 Information Management, Retention, and Information Disposal	X	X		X
SI-16 Memory Protection	X	X		
SI-20 Tainting			X	
SR-1 Supply Chain Risk Management Policy and Procedures	X	X		
SR-2 Supply Chain Risk Management Plan	X	X		
SR-3 Supply Chain Controls and Process	X	X		

SR-5 Acquisition Strategies, Tools, and Methods	X	X		
SR-6 Supplier Assessments and Reviews	X	X		
SR-8 Notification Agreements	X	X		
SR-10 Inspection of Systems or Components	X	X	X	
SR-11 Component Authenticity	X	X		
SR-12 Component Disposal	X	X		

Appendix D: Physical Access Control Guidelines

Contractors must ensure no unauthorized access to areas containing SBU data during duty and non-duty hours. This will be accomplished through use of locked containers, security containers, or limited areas inside of the secured and locked facility or office.

Securing SBU requires two barriers between the item to be protected and personnel not authorized access. These two barriers may consist of locked perimeter doors; locked interior doors; locked secured rooms; and locked security containers.

There are specific items and locations that must have special attention, as described in the next few paragraphs:

Physical Security of Computers, Electronic, and Removable Media

Because of the vast amount of information systems, electronic, optical, and other removable media (including paper), store, handle, and process, the physical security and control of information systems and electronic, optical, or other removable media (including paper) also must be addressed. Whenever possible, information system operations must be in a secure area with restricted access. In situations such as approved telework locations, remote terminals, or office work sites where all the requirements of a secure area with restricted access cannot be maintained, the equipment must receive the highest level of protection that is practical. Minimum physical security requirements must be met, such as keeping SBU data locked up when not in use. Removable media also must be labeled SBU data when they contain such information. Removable media also must be encrypted and labeled SBU data when it contains such information.

In instances where encryption is not used, the contractor must ensure that all wiring, conduits, and cabling are within the control of contractor personnel and that access to routers and network monitors are strictly controlled.

Electronic, optical, and other removable media (including paper) must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container. Good security practice requires that inventory records of electronic, optical, and other removable media be maintained for control and accountability.

Restricting Access

To assist with this requirement, SBU data must be clearly labeled as SBU data and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of protecting requirements must be used for information system screens.

Additional controls have been integrated into this document that map to guidance received from NIST. These are identified in NIST Moderate Risk Controls for Federal Information Systems.

Locked Container

A lockable container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with lockable drawers. The lock mechanism must be either a built-in key or a hasp and lock. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving or desk and credenza drawers, carts, or any other piece of office equipment designed for storing files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide protection (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

Security Containers

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks must have only two keys and strict control of the keys is mandatory; combinations must be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files.
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks.
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks, and
- Key lock "Mini Safes" properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

Locks

The lock is the most accepted and widely used security device for protecting installations and activities, personnel information, tax information, classified material, and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items must be locked when not in actual use.

However, regardless of their quality or cost, locks must be considered as delay devices only and not complete deterrents. Therefore, the locking information system must be planned and used in conjunction with other security measures. A quarterly inspection must be made on all locks to determine each locking mechanism's effectiveness, to detect tampering and to make replacement when necessary.

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must have four digits and be changed when an employee who knows the combination retires, terminates employment, transfers to another position, or at least once a year.

Combinations must be given only to those who have been granted interim or final staff-like access by Personnel Security and a need to have access to the area, room, or container and must never be written on a calendar pad, desk blotters, or any other item (even though it is carried on one's person or hidden from view).

Contractor management or designated employee must maintain combinations for door locks, safes, vaults, or other storage devices. An envelope containing the combination must be secured in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

Keys must be issued only to individuals who have been granted interim or final staff-like access by Personnel Security and a need to access an area, room, or container. An inventory must be made of all keys made and keys issued. An annual reconciliation must be done on all key records.

Safes/Vaults

A safe is a General Services Administration (GSA) approved container of Class 5 or 6, or Underwriters Laboratories (UL) Listing of TRTL-30, TRTL-60. A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, uses UL-approved vault doors, and meets GSA specifications.

Secured Interior/Secured Perimeter

Secured areas are internal areas that have been designed to prevent undetected entry by unauthorized contractor employees/persons without an IRS approved interim or final staff-like access during duty and non-duty hours.

Access to rooms or containers containing SBU information must be restricted to employees who have an IRS approved staff-like access. Secured perimeter/secured area must meet the following minimum standards:

- This area must be enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser type of partition supplemented by UL-approved electronic intrusion detection and fire detection information systems.
- There must be a manual fire alarm and evacuation system with pull boxes at each door leading out of any encapsulated areas used within the facilities.
- Unless electronic intrusion detection devices are used, all doors entering the space must be locked, and strict key or combination control must be exercised.

- In the case of a fence and gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked and have intrusion alarms.
- The space must be cleaned during duty hours in the presence of a regularly assigned employee.
- If there are louvers or vents within the secured area, such as near the door; ceiling, etc. these must be protected to detect and deter unauthorized access to the room/area, using Intrusion Detection System (IDS) methods, and
- The contractor must develop a clean desk policy that requires all employees to secure SBU data after work hours, during extended absence from work such as lunch, or when employee is not immediately working with the SBU data. The clean desk policy must be communicated to all employees.

Limited Access Areas

When designating an area as limited access, it is important to ensure that management controls of the area are in place. Examples of a limited access area include but are not limited to computer/severs rooms, telecommunication closets, processing work areas, or other areas where IRS information is readily available to any employee working within that area.

Using restricted/limited access areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access and/or disclosure of SBU data.

The Contractor must control all access points to the limited area. The entry control monitor or escort must verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort must enter the visitor's time of departure. Each limited area register must be closed out at the end of each month and reviewed by the area supervisor/manager.

Whenever visitors enter the area, the contractor must capture the following information: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

The contractor must escort visitors, including contractor employees who do not have IRS approved interim or final staff like access, and monitor visitor activity within limited processing areas.

Management or the designee must maintain an authorized list of all contractor employees with an IRS approved interim or final staff-like access that have access to information systems or areas where SBU data is stored or processed. In addition, the site must issue appropriate authorization credentials. This must not apply to those areas within the facility officially designated as publicly accessible.

It is recommended that a second level of management review the register. Each register review must include a review of the need for continued access for the employee.

Key Points:

- The area must have physical construction to enable a secured and/or limited access area, e.g., doors to prohibit unrestricted entry, construction to prevent employees from being able to access room through windows, partitioned walls, etc. Doors that provide access to secured or protected areas must have either internal door hinges or hinges that are tamper resistant.
- The number of entrances will be kept to a minimum and each entrance controlled. Only individuals assigned to the area will be provided Limited Area Access.
- A limited access area register will be maintained at the main entrance of each limited area, and all visitors will be directed to the main entrance. Each person entering a limited area, who is not assigned to the area, will be required to sign the register.
- The limited area monitor, or escort will complete the register by adding the individual's name, assigned work area, person to be contacted, purpose for entry, and time and date of entry.
- The monitor or escort will identify each visitor by comparing the name and signature entered in the register with the name and signature on some type of photo identification card (i.e., governments issued ID, driver's license) upon verification of identity, the visitor will be escorted into the Limited Area.
- Entry must be approved by the supervisor responsible for the area. The monitor or escort will enter the departure time in the register.
- Each Limited Access Area Register will be closed out at the end of each month, reviewed by the limited area first line supervisor, and forwarded to their manager. The manager will review the register and retain it for at least two years. The managerial review is designed to ensure that only authorized individuals with an official need have access to the limited areas.

These individuals are required to maintain an identifier on the badge that allows the limited access to be easily recognized, e.g., a different color background on the badge or similar mechanism.

Locking Systems for Secure and Limited Areas

Minimum requirements for locking information systems for secured areas and security rooms are high security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted high security dead bolt lock.
- A dead bolt-throw of one inch or longer.
- Double cylinder design. Cylinders are to have five or more pin tumblers, and
- Hardened inserts or be made of steel if bolt is visible when locked.

Both the key and the lock must be adequately controlled. Convenience type locking devices such as card keys, sequenced button activated locks used in conjunction with electric strikes, etc., are authorized for use only during duty hours. Keys to secured areas not in the personal custody of an authorized employee and any combinations must be stored in a security container. The number of keys or persons with knowledge of the combination to a secured area must be kept to a minimum. Keys and combinations must be given only to those

individuals, preferably supervisors, who have a frequent need to access the area after duty hours. Electronic access control systems with afterhours alarming capability can be used to secure doors to secure areas after duty hours.

Mail Processing

If IRS mail is received, the contractor must ensure that IRS incoming mail be stored in a secured area, i.e., in locked containers. All mail processing areas must have VSS coverage:

VSS

- Purpose: The purpose of a VSS is designed to reduce risk and to assist with the deterrence, detection, surveillance, and investigation of incidents or potential incidents relevant to the protection of personnel information and facilities.
- Guiding VSS Principles: In planning, implementing and/or revising of the VSS system, surveillance as it pertains to deterrence, investigation and detection must be based on the following guiding principles:

    - Risk: Ensure that appropriate visual coverage exists throughout the facility and carefully consider high risk areas. For PCA's, the area where incoming mail potentially containing remittances is opened is considered critical. Any storage of unopened mail or remittances would also be considered critical. High risk areas would include data centers/server rooms and primary ingress/egress points. Other areas would qualify as low risk. For print vendors, high risk areas would include data centers/server rooms, printing and inserting areas, primary ingress/egress points, and dock areas where large volumes of letters are stored awaiting transport. Other areas would qualify as low risk.
    - High vs. Low-Risk Areas: Avoid wide angle coverage of individual work areas where an audit trail has yet to be established. Concentrate direct coverage on individual workspace such as in extraction. Use more of a broader surveillance approach or less cameras in lower risk areas.
    - Recognition: Structure views to the extent that an individual may be personally recognized when entering/exiting interior mail processing areas even though it may be necessary to get a full shot of the doorway to guard against paper/information being passed under or somehow through the doorway.
    - Illumination: Lighting for VSS functionality must remain sufficient relative to a variety of situations such as loss of commercial power, loss of interior natural/artificial light, and nighttime surveillance. Artificial and emergency lighting must be sufficient to support surveillance and playback particularly of high-risk areas.
    - Maintenance: Optimal operations, including actual and recorded images, are achieved through regular testing and routine maintenance. Daily checks of camera views and weekly playback of recordings is required, and any identified deficiencies in the system must be addressed as soon as possible.
    - Housings: All cameras and associated cabling must be protected from tampering and vandalism. External cameras must be enclosed in tamper resistant housings.

- PTZ: In general, PTZ cameras should be used to augment fixed cameras, not replace them. Parking areas may be monitored by a combination of fixed and PTZ cameras.
- Identification: Combination intercom/camera devices must be used at entry points, particularly main entry and loading dock areas to aid in establishing identity prior to opening doors and permitting access.
- Camera Call-Up: Certain cameras such as PTZ cameras must be programmed and pre-positioned to support alarm call up in response to emergency exit doors and other critical entry/exit points such as those affiliated with the loading dock and to record such events.
- Continuous Recording: In general, these guidelines require continuous recording. However, configuration may include event recording features. Event recording is prompted by motion and/or IDS alarm activation particularly during times when the site is unattended or where surveillance involves spaces where little human activity takes place. Such a configuration may save space pertinent to recording video. Critical areas where incoming mail is opened must have continuous recording. Other high risk and low risk areas can have motion activated or event recording provided that daily camera checks and weekly playback reviews are being performed.
- Access Control: System configuration may include integration with access control. For example, while attempting to use an expired badge to gain access, a pre-programmed VSS camera will record the event (if not already in a continuous recording mode).and a guard will be alerted via monitor notification at the main guard station.

- Digital Recording: The contractor is required to provide and record surveillance of the mail processing area(s) using DVR/NVR systems, including the use of DVRs and if needed, appropriate video storage units. The DVR system must have duplex capabilities (the ability to play recorded video images while recording live images) and be supported by the necessary peripheral security equipment to ensure effectiveness and compatibility.

- Tampering: Recording and playback equipment must always be secured to prevent tampering and unauthorized use. Restricted access and usage must be managed by contractor's officials fully vetted under the IRS contract.

- Video Cassette Recording (VCR): VCR, technology and the use of VCR tapes are not acceptable due to disadvantages such as time-lapse recording.

- Virtual Real Time Recording: Recording must be conducted at a speed which will eliminate unwanted excessive stop action, or time lapse, which distracts from its usefulness including forensic value. System configuration and other factors related to digital technology may impact how well images are recorded; however, TIGTA has specified a minimum rate recording speed of 3.5 frames per second.

- Retention of Video Recordings: For PCA sites, video recordings of critical areas must be retained for one year. Other areas considered high risk must be retained for 6

months. Low risk areas must be retained for 30 days. For print vendors, high risk areas must be retained for 90 days, and low risk areas for 30 days. After the end of the retention period, image media may be destroyed or recorded over. If playback is stored on separate image media such as disks or supplemental hard drive, effective and appropriate safeguards must be in place to protect recorded images.

- Quality of Video Playback: Playback, of recorded video and the effectiveness and clarity of recorded images is critical to the design aspect of the VSS system and is of paramount importance to the Government for reasons that support accountability, prudent practice, and forensic value. Consideration must be given to the overall VSS design and system used, so factors that can degrade resolution or image quality (e.g., video compression, time lapse, recorder speed) will be minimized. Video must be able to be played back at or above the minimum recording speed of 3.5 frames per second.

- Internal or in-house playback reviews: On a weekly basis, the Contractor must ensure VSS playback is working as designed (functionality) by examining playback from at least 25% of the camera population and must be reviewed for at least one minute. Results from this review must be documented on a log.

- Weekly Video Playback Review Log must contain the following information: refer to Exhibit 6, Weekly Video Playback Review Log, for sample of log:

    - Review Date.
    - Review Name.
    - Recording Speed (if applicable).
    - DVR (if applicable) & associated camera.
    - Time/Date of video playback segment.
    - Clear Picture.
    - Imbedded date and time correct: y/n; and
    - Any other problems or concerns.

- The new Network Video Recorders (NVR) utilize “cloud computing” where video is stored on several large computer hard drives and the recording speed cannot be determined and/or is not displayed. Also, because all the cameras are input into one centralized NVR and not a traditional 16 input DVR the specific NVR cannot be determined. Therefore, these 2 required items: recording speed & specific DVR should be removed from weekly video playback review log checklist.

- Documentation and Remediation: Acceptable measures must be put in place to channel and resolve problems related to playback. In addition, these measures must be documented as procedures in media such as post orders, standard operating procedures, and/or roles and responsibilities.

- Manual Camera Review: Daily, the contractor must manually scan through all cameras to ensure connectivity, or a picture exists. This manual review is in addition to any automated or system capability designed to detect and report connectivity or

communication problems. Results from this daily scan, including any significant findings, must be documented on a log.

    - In addition, reporting and remediation efforts to timely address problems associated with this daily scan must be in place and documented.

- Matrix: A document listing cameras and related accessories must be developed.

- VSS Specifications: Upon request, the contractor must provide access to VSS manufacture specifications on all VSS related equipment and peripherals. These and other specifications, including as-built plans, diagrams, and schematics provided by the VSS design specialist or contractor must be maintained on-site and secured by a FA official.

Data Center Controls

The primary room must be a secured room/space that meets the following security requirements:

Space must be enclosed by slab-to-slab walls, which reach structural floor to structural ceiling, constructed of approved materials (normal construction material, permanent in nature such as masonry brick or drywall), that would prevent easy penetration/compromise.

If walls are not structural floor to structural ceiling, the use of wire mesh or woven wire fabric at least 10-gauge chain link fence installed above ceiling and/or under the floor to prevent unauthorized entry; or use of IDS (motion sensors) above ceiling or beneath floor to prevent unauthorized entry, is acceptable.

When IDS are used, procedures must be in place requiring that response time to alarms be 15 minutes or less.

Equipment and utilities must be locked to prevent tampering by unauthorized personnel. These keys will be controlled and limited to authorized employees. Non-IRS controls and activities must not be collocated in these rooms.

Placement of cameras is largely driven by risk or potential risk. High risk areas must be effectively covered and include the following areas:

Access to data centers must be controlled using biometric devices, or other form using two-factor authentication.

Doors: Doors that permit access (e.g., ingress/egress) to the exterior must be covered by interior cameras. Interior doors that permit access to other interior controlled areas must capture the facial view of persons as they enter and leave the space.

Controlled Rooms: Fixed camera coverage of areas such as secured storage rooms, computer rooms, security system control rooms, and main utility closets. Camera placement and

coverage must be designed and monitored so equipment, storage goods, and/or design does not interfere, diminish, or block surveillance.

The Contractor must control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. This requirement applies to both employees and visitors.

The Contractor must meet and control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output (Reference PE-5).

The Contractor must monitor physical access to the information system to detect and respond to physical security incidents (Reference PE-6).

Access logs must be maintained to identify visitors to the computer room facilities. The log must include name & organization of the person visiting; signature of the visitor; date of access; time of entry and departure, purpose of visit. Designated officials must review logs periodically (Reference PE-8).

The Contractors must control information system-related items, including hardware, firmware, software, from entering and exiting the facility and maintain appropriate records of these items (Reference PE-16).

Contractor employees must not process and/or store FTI at any sites, other than IRS approved contractor sites. Information must not be processed and/or stored from any employee's temporary and/or permanent residence, e.g., via home office or telecommuting (Reference PE-17).

Data Center Fire/Environmental Conditions

The Contractor must install a firewall to separate the main doors to computer areas and adjacent tape or other storage libraries, as necessary to protect large volumes of media.

The Contractor must control physical access to information systems telecommunications service, distribution, and or network lines within the facility that would inhibit unauthorized access, interception, or damage (Reference PE-4).

There must be an audible sounding device (alarm) that reports to a central receiving point for action/response, for each room within the firewall encapsulated area of the computer complex that will alert the complex that unauthorized persons have entered the area.

Whenever multiple devices are being tracked for any activation and/or incidents, each device must annunciate separately to the on-site protection console.

There must be a one-hour fire resistive separation of the computer (electronic equipment) area perimeter from adjoining areas to protect the electronic equipment from the damaging effects of a fire which may occur outside the equipment area.

There must be an approved Ionization system in each computer room/tape library and ionization detector heads installed above suspended ceilings (unless ceiling is fire rated), on suspended ceilings and below elevated floors, scaled to the size of the facility being safeguarded.

The Contractor must protect power equipment and power cabling for the information system from damage and destruction (Reference PE-9).

As occupants of the Contractor, the contractor must comply with all federal, state, and local codes including but not limited to National Fire Protection Association (NFPA) and National Electrical Code (NEC) requirements. Upon request, the contractor must be able to present the certification of compliance for each site (Reference PE-10).

The Contractor must provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system, in the event of a primary power source loss (Reference PE–11).

The Contractor must employ automatic emergency lighting of computer room facilities in the event of a power outage or disruption and that cover emergency exits and evacuation routes (Reference PE-12).

The Contractors must employ and maintain fire suppression equipment and detection equipment that can be activated in the event of a fire (Reference PE-13).

In addition, contractors must ensure there are systems in place to continuously monitor all electronic detection, extinguishing, and environmental and utility support systems to detect abnormal conditions.

The Contractor must install separately contained/valve wet pipe, water sprinkler system (pipe scheduled or hydraulically designed type) inside the entire firewall, encapsulated computer room and tape library areas with automatic power cut--off capability. (National Fire Protection Association (NFPA) Standard No. 13 provides details on installation of acceptable sprinkler systems).

The Contractors must regularly maintain, within acceptable levels, and monitor, the temperature and humidity within computer room and telecommunication facilities containing information systems and assets (Reference PE-14).

All air conditioning and ventilating systems must follow Section 301 of RP-1 and NFPA Standard No. 90A to ensure that the systems are designed to prevent the spread of fire, smoke, and fumes from exposed areas into the computer room or tape library.

Sprinkler water flows must contain alarms and supply valve controls.

There are floor drains or sump pumps to provide water drainage in the event of sprinkler head activation or a plumbing leak above the ceiling or under the floor.

There is a sprinkler shut-off valve (also called OS&Y) that controls the sprinkler system to the computer and/or library.

The Contractors must protect the information systems from water damage resulting from broken plumbing lines or other sources of water by ensuring that master shutoff valves are accessible, working, and known to key personnel (Reference PE-15).

The information systems must be placed to minimize damage from physical and environmental hazards and to minimize the opportunity for unauthorized access (Reference PE-18).

Appendix E: Reference

CIRCULAR NO. A-108 Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf

CIRCULAR NO. A-130 Managing Information as a Strategic Resource
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
Computer Security Act of 1987 http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt

Federal Acquisition Regulation Part 2, refer to:
http://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol1/pdf/CFR-2011-title48-vol1-sec2-101.pdf

Federal Acquisition Regulation Subpart 24.3—Privacy Training
https://www.acquisition.gov/far/subpart-24.3

Federal Information Security Management Act, refer to:
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Information Processing Standards 140-2, Security Requirements for Cryptographic Modules, refer to:
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information, and Information Systems, refer to:
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Federal Information Processing Standards 200, Minimum Security Requirements for Federal and Information Systems, refer to:
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Federal Trade Commission Financial Privacy Rule and Safeguards Rule, refer to:
http://www.gpo.gov/fdsys/pkg/FR-2000-03-01/pdf/00-4881.pdf

Gramm-Leach Bliley Act, refer to:
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Internal Revenue Code Section 26 U.S.C. § 6103, refer to:
https://www.govinfo.gov/content/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103.htm

Internal Revenue Code Section 26 U.S.C. § 7213, refer to:
26 U.S.C. 7213 - Unauthorized disclosure of information - Content Details - USCODE-2005-title26-chap75-subchapA-partI-sec7213

Internal Revenue Code Section 26 U.S.C. § 7213A, refer to: https://www.govinfo.gov/content/pkg/USCODE-2021-title26/html/USCODE-2021-title26-subtitleF-chap75-subchapA-partI-sec7213A.htm

Internal Revenue Code Section 26 U.S.C. § 7431, refer to: https://www.govinfo.gov/app/details/USCODE-2023-title26/USCODE-2023-title26-subtitleF-chap76-subchapB-sec7431?

Internal Revenue Manuals 1.15, Records, and Information Management series https://www.irs.gov/irm/part1/irm_01-015-001

OMB M-23-22: Delivering a Digital-First Public Experience https://www.whitehouse.gov/wp-content/uploads/2023/09/M-23-22-Delivering-a-Digital-First-Public-Experience.pdf?utm_source=chatgpt.com

OMB M–17–12 – Preparing for and Responding to a Breach of Personally Identifiable Information https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

National Institute of Standards and Technology Special Publication 800-18 Revision 1, Developing Security Plans for Federal Information Systems, refer to: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

National Institute of Standards and Technology Special Publication 800-53 Rev. 5, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, refer to NIST Special Publication (SP) 800- 53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations

National Institute of Standards and Technology Special Publication 800-88r2, Guidelines for Media Sanitization, refer to: SP 800-88 Rev. 2, Guidelines for Media Sanitization | CSRC

Office of Management and Budget Memorandum 07-16 https://whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2007/m07-16.pdf

Office of Management and Budget Memorandum 08-23: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2008/m08-23.pdf

Office of Management & Budget OMB Circular A-130 – Management of Federal Information Resources, refer to https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

Privacy Act of 1974, refer to: https://www.dodig.mil/Portals/48/Documents/Programs/Privacy%20Program/pa1974.pdf?utm_source=chatgpt.com

Sarbanes-Oxley Act, refer to:
http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

Section 552a of Title 5, United States Code